

# The polynomial degree of the Grassmannian $\mathcal{G}_{1,n,2}$

R. SHAW

r.shaw@hull.ac.uk

Department of Mathematics, University of Hull, Hull HU6 7RX, United Kingdom

N. A. GORDON

n.a.gordon@hull.ac.uk

Department of Computer Science, University of Hull, Hull HU6 7RX, United Kingdom

## Abstract

For a subset  $\psi$  of  $\text{PG}(N, 2)$  a known result states that  $\psi$  has polynomial degree  $\leq r$ ,  $r \leq N$ , if and only if  $\psi$  intersects every  $r$ -flat of  $\text{PG}(N, 2)$  in an odd number of points. Certain refinements of this result are considered, and are then applied in the case when  $\psi$  is the Grassmannian  $\mathcal{G}_{1,n,2} \subset \text{PG}(N, 2)$ ,  $N = \binom{n+1}{2} - 1$ , to show that for  $n < 8$  the polynomial degree of  $\mathcal{G}_{1,n,2}$  is  $\binom{n}{2} - 1$ .

Keywords: polynomial degree, subsets of  $\text{PG}(N, 2)$ , Grassmannian  $\mathcal{G}_{1,n,2}$

AMS Classification: 51E20, 05C90, 11G25, 14M15

## 1 Introduction

### 1.1 The $\text{GF}(2)$ -spaces $F(V)$ , $F(S)$ , $F_r$ , $C_r$ , $\bar{C}_r$

Let  $\text{PG}^{(r)}(N, 2)$  denote the set of all the  $r$ -flats of  $\text{PG}(N, 2) = \mathbb{P}(V(N+1, 2))$ . We also put  $S = \text{PG}^{(0)}(N, 2)$  for the set of points of  $\text{PG}(N, 2)$ . Throughout we will identify  $S$  with the nonzero vectors  $V \setminus \{0\}$  of the vector space  $V = V_{N+1} = V(N+1, 2)$ . Consider the vector space  $F(V)$  over  $\text{GF}(2)$  consisting of all functions  $V \rightarrow \text{GF}(2)$ . Then  $\dim F(V) = |V| = 2^{N+1}$ . Each subset  $\psi \subseteq V$  gives rise to an element of  $F(V)$ , namely the characteristic function of  $\psi$ , which we denote either by  $\chi(\psi)$  or by  $\chi_\psi : \chi_\psi(x) = 1$  if  $x \in \psi$ , and  $\chi_\psi(x) = 0$  if  $x \notin \psi$ . Indeed every element  $f \in F(V)$  is of this kind, since  $f = \chi_\psi$  where  $\psi$  is the support of  $f$ . In the case when  $\psi$  is a singleton set  $\{a\}$ ,  $a \in V$ , we put  $\chi_a := \chi_{\{a\}}$ . Let  $\langle \cdot, \cdot \rangle$  denote the usual non-degenerate scalar product on  $F(V)$ :  $\langle f_1, f_2 \rangle = \sum_{x \in V} f_1(x)f_2(x)$ . Then  $\{\chi_a\}_{a \in V}$  is an orthonormal basis for  $F(V)$ . In fact, rather than  $F(V)$ , our main focus is on the vector space  $F(S)$  over  $\text{GF}(2)$  consisting of all functions  $S \rightarrow \text{GF}(2)$ ; so  $\dim F(S) = |S| = 2^{N+1} - 1$ . *In fact we will consider  $F(S)$  to be a subspace of  $F(V)$* , by identifying an element  $f \in F(S)$  with that element  $f_0 \in F(V)$  such that  $f_0(0) = 0$  and  $f_0(a) = f(a)$  for  $a \in S$ . Then  $F(V)$  has the orthogonal direct sum decomposition  $F(V) = \langle \chi_0 \rangle \perp F(S)$ .

Upon choosing a basis  $\mathcal{B} = \{e_1, e_2, \dots, e_{N+1}\}$  for  $V$  an element  $x \in V$  may be viewed as an  $(N+1)$ -tuple  $(x_1, x_2, \dots, x_{N+1}) \in \text{GF}(2)^{N+1}$ , in terms of coordinates  $x_i \in \text{GF}(2)$ . The basis  $\mathcal{B}$  for  $V$  gives rise to an associated *monomial basis*  $\mathcal{M}$  for  $F(S)$ , namely

$$\mathcal{M} = \Xi_1 \cup \Xi_2 \cup \dots \cup \Xi_{N+1}, \quad \text{where } \Xi_r = \{x_{i_1}x_{i_2}\dots x_{i_r}\}_{1 \leq i_1 < i_2 < \dots < i_r \leq N+1}, \quad (1.1)$$

and by adding the constant function 1 to  $\mathcal{M}$  we obtain a basis  $\mathcal{M}' := \{1\} \cup \mathcal{M}$  for  $F(V) = \langle 1 \rangle \oplus F(S)$ . To see that  $\mathcal{M}'$  is indeed a basis, first observe that we clearly have

$$\chi_0(x) = \prod_{i=1}^{N+1} (1 + x_i), \quad \chi_a(x) = \chi_0(a + x), \quad (1.2)$$

and so each element of the basis  $\{\chi_a\}_{a \in V}$  has an expansion in terms of the elements of  $\mathcal{M}'$ . Secondly note that  $|\mathcal{M}'| = \sum_{r=0}^{N+1} \binom{N+1}{r} = 2^{N+1} = \dim F(V)$ . Incidentally in the basis  $\mathcal{B}$  every non-constant monomial function coincides with one belonging to  $\mathcal{M}$ , since over  $\text{GF}(2)$  we have  $(x_i)^h = x_i$  for  $h > 0$ .

*From now on we confine attention to the space  $F(S)$  rather than to  $F(V)$ .* Note that the scalar product on  $F(S)$ , given by  $\langle f_1, f_2 \rangle = \sum_{x \in S} f_1(x)f_2(x)$ , is non-degenerate. For  $r > 0$ , let  $F_r = F_r(S)$  denote the subspace of  $F(S)$  which consists of functions  $f$  expressible as a polynomial function  $f(x_1, x_2, \dots, x_{N+1})$  with  $\deg f \leq r$  and  $f(0) = 0$ ; we put  $F_0 := \{0\}$ . The subspaces  $F_r$  are thus nested:

$$\{0\} = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_N \subset F_{N+1} = F(S), \quad (1.3)$$

with  $F_r$ ,  $r \geq 1$ , possessing the monomial basis  $\mathcal{M}_r$  where

$$\mathcal{M}_r = \Xi_1 \cup \Xi_2 \cup \dots \cup \Xi_r, \quad 1 \leq r \leq N+1. \quad (1.4)$$

The subspace  $F_r$  thus has dimension

$$\dim(F_r) = |\mathcal{M}_r| = \sum_{s=1}^r |\Xi_s| = \sum_{s=1}^r \binom{N+1}{s}. \quad (1.5)$$

Observe that  $\Xi_{N+1}$  consists of the single monomial  $m_{N+1} := x_1x_2\dots x_{N+1}$ . Now from (1.2) the expansions of the characteristic functions  $\chi_a$ ,  $a \in S$ , along the basis  $\mathcal{M}$  all involve this monomial  $m_{N+1}$ . Consequently, for a subset  $\psi$  of  $S$ ,

- (i)  $\chi(\psi) \in F_N$  if and only if  $|\psi|$  is even
- (ii)  $\chi(\psi) \in F_{N+1} \setminus F_N$  if and only if  $|\psi|$  is odd. (1.6)

Concerning the characteristic functions  $\chi_\psi = \chi(\psi) \in F(S)$  of subsets  $\psi \subseteq S$ , take note that for any subsets  $\phi, \psi$  of  $S$  we have

$$\langle \chi_\phi, \chi_\psi \rangle = \begin{cases} 0, & \text{if } |\phi \cap \psi| \text{ is even,} \\ 1, & \text{if } |\phi \cap \psi| \text{ is odd.} \end{cases} \quad (1.7)$$

If  $\psi^c$  denotes the complement *within the set*  $S$  of  $\psi$  then observe that

$$\chi(\psi) + \chi(\psi^c) = I, \quad (1.8)$$

where  $I(= \chi(S))$  denotes that element of  $F(S)$  such that  $I(x) = 1$  for all  $x \in S$ . We may immediately check that  $I$  has the coordinate expression

$$I(x) = 1 + \prod_{i=1}^{N+1} (1 + x_i) = \sum_i x_i + \sum_{i < j} x_i x_j + \dots + x_1 x_2 \dots x_{N+1}. \quad (1.9)$$

From (1.7) it follows that for any subset  $\psi$  of  $S$  we have  $\langle \chi(\psi), I \rangle = 0$  or 1 according as  $|\psi|$  is even or odd, (and in particular  $\langle I, I \rangle = 1$ ). Hence note the property

$$\langle \chi(X^c), I \rangle = 0 \text{ for any } r\text{-flat } X, \ r \geq 0. \quad (1.10)$$

**Definition 1.1** For  $0 \leq r \leq N$  define subspaces  $C_r$  and  $\bar{C}_r$  of  $F(S)$  by

$$C_r = \prec \chi(X^c) \succ_{X \in \text{PG}^{(r)}(N,2)}, \quad \bar{C}_r = \prec \chi(X) \succ_{X \in \text{PG}^{(r)}(N,2)}. \quad (1.11)$$

Note therefore that  $\bar{C}_0 = \prec \chi_a \succ_{a \in S} = F(S)$ , and that  $C_0$  consists of the characteristic functions of all even subsets of  $S$ , whence, from (1.6),  $C_0 = F_N$ . Note also that  $C_N = \{0\}$ ,  $\bar{C}_N = \prec I \succ$ , and  $C_{N-1} = F_1$ .

Now that we are confining our attention to the space  $F(S)$ , and to its subspaces, the notation  $W^\perp$  will be used for that subspace of  $F(S)$  which is orthogonal to the subspace  $W$  of  $F(S)$ . Since the scalar product on  $F(S)$  is non-degenerate note therefore that for any subspace  $W$  of  $F(S)$

$$(W^\perp)^\perp = W \quad \text{and} \quad \dim W + \dim(W^\perp) = 2^{N+1} - 1. \quad (1.12)$$

Since for any  $r$ -flat  $X$ ,  $r \geq 0$ , we have, see (1.10),  $\chi(X^c) \in \prec I \succ^\perp$ , it follows that  $C_r \subseteq \prec I \succ^\perp$  for each  $r = 0, 1, \dots, N$ . Upon recalling (1.8) we thus see that the space  $\bar{C}_r$  has the orthogonal direct sum decomposition

$$\bar{C}_r = \prec I \succ \perp C_r, \quad r = 0, 1, \dots, N-1. \quad (1.13)$$

## 1.2 The polynomial degree of a subset $\psi$ of $S$

If a particular subset  $\psi$  of  $S$  is singled out for investigation then we let  $Q = Q_\psi := \chi(\psi^c)$  be the characteristic function of its complement  $\psi^c$ . Then  $\psi$  has equation  $Q(x) = 0$ . If  $Q \in F_r \setminus F_{r-1}$  we will say that  $\psi$  has *polynomial degree*  $r$ , and we write  $\deg Q = r$  for the degree of  $Q$ . (Here  $\deg Q$  is the *reduced* degree of  $Q$ ; if  $\deg Q = r$  then of course, see (1.3),  $Q \in F_s$  for each  $s \geq r$ .) Recall that  $C_0 = F_N$  and that  $C_0$  consists of the characteristic functions of all the even subsets of  $S$ . Consequently if  $\psi$  is an odd subset of  $S$  (and so  $\psi^c$  is an even subset) then  $\psi$  has polynomial degree  $\leq N$ . Now  $\chi(\psi) + \chi(\psi^c) = I$ , and, see (1.9),  $\deg I = N + 1$ ; *so an even subset always has polynomial degree  $N + 1$* . The chief interest therefore lies, as in section 2.2, with odd subsets  $\psi$  of  $S$ .

**Remark 1.2** *The polynomial degree of a subset  $\psi$  of  $\text{PG}^{(0)}(N, q)$  may be similarly defined. However for  $q > 2$  there are in addition to  $Q = \chi(\psi^c)$  many other polynomial functions  $P$  whose support is  $\psi^c$ , and so  $\psi$  has many different equations  $P(x) = 0$ .*

*Plan.* In section 2 we outline some methods which may be employed in the determination of the polynomial degree of a general subset  $\psi \subset S$ . From section 3 onwards, we concentrate on the particular case where  $\psi$  is the Grassmann image  $\mathcal{G}_{1,n,2} \subset \text{PG}^{(0)}(N, 2)$ ,  $N = \binom{n+1}{2} - 1$ , of the lines of  $\text{PG}(n, 2)$ . To these ends we first describe some relevant background results. Most of these results are essentially well-known; indeed they are the  $q = 2$  versions of more general results obtained, for example, in [7]. However the  $q = 2$  results in theorems 1.8 and 1.9 may perhaps be rather less well-known: see section 1.2.2(iv).

### 1.2.1 Some background results

**Lemma 1.3** *Let  $X$  be an  $(N - r)$ -flat in  $\text{PG}(N, 2)$  which is the intersection of the  $r$  hyperplanes  $f_1(x) = 0, \dots, f_r(x) = 0$ , where the  $f_i$  are elements of the dual  $\tilde{V} = \tilde{V}_{N+1}$  of  $V$ . Then*

$$\begin{aligned} \chi(X^c) &= 1 + \prod_{i=1}^r (1 + f_i) \\ &= \sum_i f_i + \sum_{i < j} f_i f_j + \sum_{i < j < k} f_i f_j f_k + \dots + f_1 f_2 \dots f_r. \end{aligned} \quad (1.14)$$

**Proof.**  $1 + \prod_{i=1}^r (1 + f_i)$  equals 1 except when  $f_1 = f_2 = \dots = f_r = 0$ . ■ Observe that the previous expression (1.9) may be viewed as the special case  $r = N + 1$ ,  $X^c = S$  of (1.14).

**Lemma 1.4** (i)  $\prec I \succ = \bar{C}_N \subseteq \bar{C}_{N-1} \subseteq \dots \subseteq \bar{C}_1 \subseteq \bar{C}_0 = F(S)$ .

(ii)  $\{0\} = C_N \subseteq C_{N-1} \subseteq \dots \subseteq C_1 \subseteq C_0 = \prec I \succ^\perp$ .

**Proof.** If  $X$  is an  $(r + 1)$ -flat, then  $\chi(X) = \sum_{i=1}^3 \chi(Y_i)$ , where  $Y_1, Y_2, Y_3$  are the three  $r$ -flats in  $X$  which contain a(ny) chosen  $(r - 1)$ -flat of  $X$ ; so  $\bar{C}_{r+1} \subseteq \bar{C}_r$ . Because of (1.13), the nesting (ii) follows from that in (i). ■

**Theorem 1.5** *For  $r = 1, 2, \dots, N$  we have  $C_{N-r} = F_r$ .*

**Proof.** From (1.14) it follows that  $C_{N-r} \subseteq F_r$ ,  $r = 1, 2, \dots, N$ . To show that  $F_r \subseteq C_{N-r}$ , suppose that  $F_s \subseteq C_{N-s}$  holds for  $s < r$ . We have a basis for an inductive argument, since  $F_1 = C_{N-1}$ . Now for any  $f_i \in \tilde{V} \setminus \{0\}$  we see from (1.14) that  $f_1 f_2 \dots f_r \in C_{N-r} + F_{r-1}$  and hence, by our hypothesis, that  $f_1 f_2 \dots f_r \in C_{N-r} + C_{N-r+1}$ . But elements of the form  $f_1 f_2 \dots f_r$  span  $F_r$ , and, lemma 1.4(ii),  $C_{N-r+1} \subseteq C_{N-r}$ , whence  $F_r \subseteq C_{N-r}$ . ■

Bearing in mind the preceding theorem it proves convenient to adopt the alternative notation  $\bar{F}_r$  for the subspace  $\bar{C}_{N-r} = \prec I \succ^\perp C_{N-r}$  of  $F(S)$ . Thus

$$\bar{F}_r = \prec I \succ^\perp F_r, \quad r = 0, 1, \dots, N. \quad (1.15)$$

**Theorem 1.6** *The following hold for  $r = 0, 1, \dots, N$ :*

$$(C_r)^\perp = \bar{C}_{N-r} = \bar{F}_r; \quad (F_r)^\perp = \bar{F}_{N-r} = \bar{C}_r. \quad (1.16)$$

**Proof.** If  $X$  is any  $(N-r)$ -flat and  $Y$  is any  $r$ -flat then  $X \cap Y$  is a  $k$ -flat for some  $k \geq 0$ . Hence  $|X^c \cap Y|$  is even, whence  $\langle \chi(X^c), \chi(Y) \rangle = 0$ . So the subspace  $C_{N-r} = F_r$  is orthogonal to the subspace  $\bar{C}_r = \bar{F}_{N-r} = \prec I \succ \perp F_{N-r}$ . But from (1.5) the dimensions of these two subspaces sum to  $2^{N+1} - 1 = \dim(F(S))$ , whence  $(F_r)^\perp = \bar{F}_{N-r}$ . The rest of (1.16) follows from theorem 1.5. ■

Since an even subset always has polynomial degree  $N+1$ , in the following theorem we confine attention to odd subsets.

**Theorem 1.7** *For  $r \leq N$ , an odd subset  $\psi$  of  $S$  has polynomial degree  $\leq r$ , if and only if  $\psi$  meets each  $r$ -flat of  $\text{PG}(N, 2)$  in an odd number of points.*

**Proof.** (Cf. [8].) By the result  $(F_r)^\perp = \bar{C}_r$  in theorem 1.6,  $\chi(\psi^c) \in F_r$  if and only if, for each  $r$ -flat  $X$ ,  $\langle \chi(\psi^c), \chi(X) \rangle = 0$ , that is, since  $|\psi|$  is odd and using equation (1.7), if and only if  $|\psi \cap X|$  is odd. ■

For the next theorem we need some further notation. With respect to a choice of basis  $\{e_1, e_2, \dots, e_{N+1}\}$  for  $V_{N+1}$ , let  $X_{i_1 i_2 \dots i_s}$  denote that  $(N-s)$ -flat with coordinate equation  $x_{i_1} = x_{i_2} = \dots = x_{i_s} = 0$ , and let  $Y(j_1, j_2, \dots, j_s)$  denote the  $(s-1)$ -flat  $\langle e_{j_1}, e_{j_2}, \dots, e_{j_s} \rangle$ . Observe that if  $\{j_1, j_2, \dots, j_{N+1-s}\} = \{1, 2, \dots, N+1\} \setminus \{i_1, i_2, \dots, i_s\}$  then

$$X_{i_1 i_2 \dots i_s} = Y(j_1, j_2, \dots, j_{N+1-s}). \quad (1.17)$$

**Theorem 1.8** (Simplex Basis) *Set  $\mathcal{F}_s = \{\chi_{i_1 \dots i_s}\}_{1 \leq i_1 < i_2 < \dots < i_s \leq N+1}$  where  $\chi_{i_1 \dots i_s} := \chi(X_{i_1 \dots i_s}^c)$ . Then, for  $1 \leq r \leq N$ ,*

$$\mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots \cup \mathcal{F}_r \quad (1.18)$$

*is a basis for  $C_{N-r}$  (and hence is a basis for  $F_r$ ).*

**Proof.** This follows from (1.4) upon noting from (1.14) that the element  $\chi_{i_1 i_2 \dots i_s}$  of  $C_{N-s}$  differs from  $x_{i_1} x_{i_2} \dots x_{i_s}$  by elements of  $F_{s-1} = C_{N-s+1}$ . ■

From (1.17) observe that *the elements of  $\mathcal{F}_s$  are in bijective correspondence with the faces of the simplex of reference of projective dimension  $N-s$ .*

**The action of  $\text{GL}(N+1, 2)$ .**

For  $A \in \text{GL}(V_{N+1}) = \text{GL}(N+1, 2)$  let  $U_A \in \text{GL}(F(S))$  be defined by  $(U_A f)(x) = f(A^{-1}x)$ ,  $f \in F(S)$ . Under this natural action  $U$  of  $\text{GL}(N+1, 2)$  the space  $F(S)$  has the invariant decomposition  $F(S) = \prec I \succ \oplus F_N = \prec I \succ \oplus C_0$ . However under this action the space  $F_N$  is indecomposable, but instead has the reduction given by the composition series in the next theorem.

**Theorem 1.9** (i) For  $r = 1, 2, \dots, N + 1$  there exists a natural linear isomorphism  $\rho_r : \wedge^r \tilde{V} \rightarrow F_r/F_{r-1}$  satisfying

$$\rho_r(f_1 \wedge \dots \wedge f_r) = f_1 \dots f_r \pmod{F_{r-1}}, \quad \text{for all } f_i \in \tilde{V}_{N+1}. \quad (1.19)$$

(ii) Under the natural action  $U$  of  $\text{GL}(N + 1, 2)$

$$\{0\} = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_N \subset F_{N+1} = F(S) \quad (1.20)$$

is a composition series for  $F(S)$ .

**Proof.** (i) The r.h.s. of (1.19) lies in  $F_r/F_{r-1}$  and is a multilinear function of  $f_1, \dots, f_r$ . Moreover it is also alternating, since  $f_1 \dots f_r \in F_{r-1}$  whenever  $f_i = f_j$  for some  $i \neq j$ . Hence a linear map  $\rho_r$  satisfying (1.19) exists. Moreover  $\rho_r$  is surjective, since elements of the form  $f_1 \dots f_r$  span  $F_r$ . Finally note from (1.4) that  $\dim(F_r/F_{r-1}) = |\Xi_r| = \binom{N+1}{r}$ , which equals  $\dim(\wedge^r \tilde{V})$ ; so each  $\rho_r$  is an isomorphism.

(ii)  $\text{GL}(N+1, 2)$  acts irreducibly upon  $\wedge^r \tilde{V}$  and hence upon each quotient space  $F_r/F_{r-1} \cong \wedge^r \tilde{V}$ . ■

### 1.2.2 Commentary

(i) The function  $I(x)$  is the only nonzero  $\text{GL}(N + 1, 2)$ -invariant function in  $F(S)$ . However there do exist (related)  $\text{GL}(N + 1, 2)$ -invariant functions  $I_2(x, y)$ ,  $I_3(x, y, z)$ ,  $\dots$ , of several vector variables, and these are of use in certain contexts. See [10], [5]; see also [7] for their  $\text{PG}(N, q)$  generalizations.

(ii) The notation  $C_r$  and  $\tilde{C}_r$  for the subspaces in (1.11) agrees with that in [7]. *However a cautionary remark is in order:* our present  $W^\perp$  is denoted  $W^*$  in [7]; moreover the notation  $W^\perp$  in [7] is used to denote the orthogonal complement *within*  $C_0$  of a subspace  $W \subseteq C_0$ .

(iii) If we employ  $\{\chi_a\}_{a \in V}$  as basis for  $F(V)$  then  $\prec 1 \succ \oplus F_r$  is the Reed-Muller code  $\mathcal{R}(r, N + 1)$ , of length  $2^{N+1}$  and dimension  $\sum_{s=0}^r \binom{N+1}{s}$ . Using  $\{\chi_a\}_{a \in S}$  as basis for  $F(S)$  then, from its definition (1.1),  $\tilde{C}_r$  is the binary code of the design of points and  $r$ -flats of  $\text{PG}(N, 2)$ , and, since  $\tilde{C}_r = \prec I \succ \oplus F_{N-r}$ , it is the punctured Reed-Muller code  $\mathcal{R}(N - r, N + 1)^*$ , of length  $2^{N+1} - 1$  and dimension  $\sum_{s=0}^{N-r} \binom{N+1}{s}$ . See [1, Chapter 5].

(iv) The results in theorems 1.8 and 1.9 were uncovered some time ago by one of the present authors — albeit, see [9, Section 2], in the course of some researches into Clifford algebras! (However section 2 of [9] is free of these Clifford algebra concerns.)

## 2 Finding the polynomial degree of a subset $\psi \subset S$

### 2.1 Algebraic approaches

Given a subset  $\psi \subset S$  then  $\chi(\psi^c) = I + \chi(\psi) = I + \sum_{a \in \psi} \chi_a$ , and so, by equation (1.8),  $Q = Q_\psi := \chi(\psi^c)$  is the polynomial function

$$Q(x) = I(x) + \sum_{a \in \psi} \prod_{i=1}^{N+1} (1 + a_i + x_i). \quad (2.1)$$

However the task of finding the polynomial degree of  $\psi$  by determining  $Q$  from this expression is not usually an attractive one, even by computer. For example, in the case when  $\psi$  is the Grassmannian  $\mathcal{G}_{1,7,2} \subset \text{PG}(27, 2)$ , the summation in (2.1) consists of  $|\mathcal{G}_{1,7,2}| = 10,795$  terms, each term being the product of 28 factors  $1 + a_i + x_i$ , and so, before simplification, each of the 10,795 terms in the summation expands to produce  $3^{28}$  terms.

In cases where  $\psi$  is known to be the set of points which simultaneously satisfy several polynomial equations  $g_i(x) = 0$ , with  $g_i(0) = 0$ , then an alternative explicit determination of  $Q$  is available; namely (cf. lemma 1.3)

$$\begin{aligned} Q &= 1 + \prod_{i=1}^r (1 + g_i) \\ &= \sum_i g_i + \sum_{i < j} g_i g_j + \sum_{i < j < k} g_i g_j g_k + \dots + g_1 g_2 \dots g_r. \end{aligned} \quad (2.2)$$

In particular  $\deg Q$  is determined after reduction, replacing  $(x_i)^{a_i}$  for  $a_i > 1$  by  $x_i$ . However it should be noted that even in cases where a set of equations  $g_i(x) = 0$  is known, the computation of  $Q$  via (2.2) is a formidable task, and is often not feasible, even by computer. See section 4.1.

Rather than this algebraic approach to finding the polynomial degree, in the present paper we will be chiefly interested in seeking *geometric approaches*, involving the relation of  $\psi$  to the flats of  $\text{PG}(N, 2)$ , in the hope that this may prove a more amenable approach.

### 2.2 Geometric approaches

Let  $\psi$  be an odd subset of  $S = \text{PG}^{(0)}(N, 2)$ . In this section we consider applying the results in section 1.2.1 to provide information concerning the polynomial degree of  $Q = Q_\psi := \chi(\psi^c)$ . For condition C.4 in the next theorem, if  $G = G(\psi)$  is the subgroup of  $\text{GL}(N + 1, 2)$  which stabilizes  $\psi$ , and if the  $G$ -orbits of  $r$ -flats of  $\text{PG}(N, 2)$  are  $\Omega_r(i), i = 1, 2, \dots$ , then let  $X_r(i)$  be a representative of  $\Omega_r(i)$ . For condition C.5 we choose a basis  $\{e_1, \dots, e_{N+1}\}$  for  $V_{N+1}$  and, see eq. (1.17), employ the  $r$ -flats  $X_{i_1 i_2 \dots i_{N-r}} = Y(j_1, j_2, \dots, j_{r+1})$ . For condition C.6, if  $G_0 = G_0(\psi)$  is the subgroup of  $G$  which stabilizes the basis  $\{e_1, \dots, e_{N+1}\}$ , and if  $\Phi_r(i), i = 1, 2, \dots$  are the  $G_0$ -orbits of those  $r$ -flats of the kind  $Y(j_1, j_2, \dots, j_{r+1})$ , then let  $Y_r(i)$  be a representative of  $\Phi_r(i)$ .

**Theorem 2.1** *If  $\psi$  is an odd subset of  $S$  then the polynomial  $Q = Q_\psi$  will lie in  $F_r$  if any one of the following conditions is satisfied:*

*C.1. there exist a family  $\Psi$  of  $(N - r)$ -flats of  $\text{PG}(N, 2)$  such that*

$$Q = \sum_{X \in \Psi} \chi(X^c); \quad (2.3)$$

*C.2. every  $r$ -flat  $X$  intersects  $\psi$  in an odd number of points;*

*C.3. there exists a family  $\Psi$  of  $r$ -flats of  $\text{PG}(N, 2)$  such that each  $X \in \Psi$  meets  $\psi$  in an odd number of points, and such that  $\prec \{\chi(X^c)\}_{X \in \Psi} \succ = C_r$ ;*

*C.4. each of the  $r$ -flats  $X_r(i), i = 1, 2, \dots$  has odd intersection with  $\psi$ ;*

*C.5.  $Q \in F_{r+1}$  and each of the  $r$ -flats  $Y(j_1, j_2, \dots, j_{r+1})$  has odd intersection with  $\psi$ ;*

*C.6.  $Q \in F_{r+1}$  and each of the  $r$ -flats  $Y_r(i), i = 1, 2, \dots$  has odd intersection with  $\psi$ .*

**Proof.** First consider conditions C.1 - C.4. Each term  $\chi(X^c)$  in (2.3) lies in  $C_{N-r}$ ; so if C.1 applies then  $Q \in C_{N-r} = F_r$ . By theorem 1.7 condition C.2 implies that  $Q \in F_r$ . Conditions C.3 and C.4 apply, since either of them entails condition C.2.

Concerning conditions C.5 and C.6, given  $Q \in F_{r+1}$  it follows from  $(F_{r+1})^\perp = \bar{C}_{r+1}$  that  $Q$  is orthogonal to each element of the basis  $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots \cup \mathcal{F}_{N-r-1}$  for  $C_{r+1}$ . Given also that  $\psi$  meets each  $r$ -flat  $Y(j_1, j_2, \dots, j_{r+1})$  in an odd number of points, it follows that  $Q$  is also orthogonal to each element of  $\mathcal{F}_{N-r}$ ; further, since  $|\psi|$  is odd,  $\langle Q, I \rangle = 0$ . Hence  $Q$  is orthogonal to each element of the basis  $\{I\} \cup \mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots \cup \mathcal{F}_{N-r}$  for  $\bar{C}_r$ , and so  $Q \in (\bar{C}_r)^\perp = F_r$ . Finally condition C.6 applies, since it entails C.5. ■

**Theorem 2.2** *Let  $\psi$  be an odd subset of  $S = \text{PG}^{(0)}(N, 2)$ , and suppose that both of the following hold:*

*(a)  $\psi$  satisfies one of the conditions C.1 - C.6 of theorem 2.1;*

*(b) there exists an  $(r-1)$ -flat  $X$  which meets  $\psi$  in an even number of points.*

*Then  $\psi$  has polynomial degree  $r$ .*

**Proof.** Because  $\psi$  satisfies one of the conditions C.1 - C.6 we know from theorem 2.1 that  $Q_\psi \in F_r$ . But from (b) it follows from theorem 1.7 that  $Q_\psi \notin F_{r-1}$ . Hence  $\psi$  has polynomial degree  $r$ . ■

**Remark 2.3** *(i) Since  $\chi(\psi) + \chi(\psi^c) = I$ , condition C.1 of theorem 2.1 is equivalent to the existence of a family  $\Psi$  of  $(N - r)$ -flats of  $\text{PG}(N, 2)$  such that*

$$\begin{aligned} \text{either } \quad & \chi(\psi) = \sum_{X \in \Psi} \chi(X), \quad \text{where } |\Psi| \text{ is odd,} \\ \text{or } \quad & \chi(\psi) = I + \sum_{X \in \Psi} \chi(X), \quad \text{where } |\Psi| \text{ is even.} \end{aligned}$$

*(ii) In condition C.4 we could instead let the  $X_r(i)$  be representatives of the  $G_1$ -orbits of  $r$ -flats of  $\text{PG}(N, 2)$  for any choice of subgroup  $G_1$  of  $G$ . But*

of course using a smaller group will usually involve more orbits and so more work to do in applying condition C.4.

(iii) In the next section, where we consider the case when  $\psi$  is the Grassmannian  $\mathcal{G}_{1,n,2} \subset \text{PG}(N, 2)$ ,  $N = \binom{n+1}{2} - 1$ , our chief weapon will be that of condition C.2 and theorem 1.7, namely that  $\psi$  has polynomial degree  $\leq r$  if and only if  $\psi$  intersects every  $r$ -flat of  $\text{PG}(N, 2)$  in an odd number of points. (Cf. [8].) However we will also need the refinements of this result, see conditions C.5, C.6, which arise from the use of the simplex of reference basis (1.18) in theorem 1.8.

### 3 The polynomial degree of the Grassmannian $\mathcal{G}_{1,n,2}$

For  $V_{n+1} = V(n+1, 2)$  the bivector space  $\wedge^2 V_{n+1}$  has vector space dimension  $\binom{n+1}{2}$ . From now on we will be dealing with the associated projective space  $\mathbb{P}(\wedge^2 V_{n+1}) = \text{PG}(N, 2)$ , where  $N := N_n = \binom{n+1}{2} - 1$ . In particular, for  $n \geq 3$ , we will be interested in the Grassmannian  $\mathcal{G}_{1,n,2} \subset \text{PG}^{(0)}(N, 2)$ , which consists of the Grassmann images  $m = a \wedge b$  of the lines  $\mu = \langle a, b \rangle$  of  $\text{PG}(n, 2) = \mathbb{P}V_{n+1}$ . Observe, since  $|\mathcal{G}_{1,n,2}| = \frac{1}{3}(2^{n+1} - 1)(2^n - 1)$  is odd, that we may take  $\psi = \mathcal{G}_{1,n,2}$  in conditions C.1 - C.7 and theorem 2.2 of section 2.2.

The natural action of  $A \in \text{GL}(n+1, 2)$  upon  $V_{N+1} := \wedge^2 V_{n+1}$  is by  $T_A = \wedge^2 A : a \wedge b \mapsto Aa \wedge Ab$ . Now, for  $n > 3$ , the subgroup  $G(\mathcal{G}_{1,n,2})$  of  $\text{GL}(N+1, 2)$  which stabilizes  $\mathcal{G}_{1,n,2}$  is the isomorphic image under  $T$  of  $\text{GL}(n+1, 2)$ . Consequently the function space  $F(S)$ ,  $S := \text{PG}^{(0)}(N, 2)$  will be viewed as a  $\text{GL}(n+1, 2)$ -space under the action  $L$  defined by

$$(L_A f)(x) = f(T_A^{-1}x), \quad A \in \text{GL}(n+1, 2), \quad x \in S. \quad (3.1)$$

It is easy to see that the maximal flats which are internal to  $\mathcal{G}_{1,n,2}$  are of two kinds, namely:

(i) *Latin*  $(n-1)$ -flats  $\text{St}(a)$ ,  $a \in \text{PG}^{(0)}(n, 2)$ , of the form

$$\text{St}(a) := \{a \wedge x \mid x \in \text{PG}^{(0)}(n, 2) \setminus \{a\}\}; \quad (3.2)$$

(ii) *Greek planes*  $P(\alpha)$  which consist of the Grassmann images of the lines of a plane  $\alpha \subset \text{PG}^{(0)}(n, 2)$ .

In the following we set  $Q_{1,n,2} = \chi((\mathcal{G}_{1,n,2})^c)$ , and we also write

$$N_n = n + d_n, \quad \text{where } d_n := N_n - n = \binom{n}{2} - 1. \quad (3.3)$$

Note therefore, from theorem 1.5,

$$F_{d_n} = C_n, \quad F_n = C_{d_n}. \quad (3.4)$$

### 3.1 Some general results, and the main conjecture

**Theorem 3.1** *The polynomial degree of  $\mathcal{G}_{1,n,2}$  is  $\leq d_n + 1$ .*

**Proof.** Consider  $f := \sum_{a \in \text{PG}^{(0)}(n,2)} \chi(\text{St}(a))$ . Then  $f(x) = 0$  for  $x \in \mathcal{G}_{1,n,2}^c$ , because  $\text{St}(a) \subset \mathcal{G}_{1,n,2}$ ; also  $f(m) = 3 = 1$  for  $m \in \mathcal{G}_{1,n,2}$ , because the image  $m$  of a line  $\mu$  belongs to precisely three Latin flats, namely  $\text{St}(a)$  for the three points  $a \in \mu$ . Hence

$$\chi(\mathcal{G}_{1,n,2}) = \sum_{a \in \text{PG}^{(0)}(n,2)} \chi(\text{St}(a)). \quad (3.5)$$

Hence, by C.1 of theorem 2.1 and remark 2.3(i),  $Q_{1,n,2} \in F_{d_n+1}$ . ■

**Theorem 3.2** *The polynomial degree of  $\mathcal{G}_{1,n,2}$  is  $\geq d_n$ .*

**Proof.** In [3] Cooperstein proved the existence of a  $(d_n - 1)$ -flat  $X$  external to  $\mathcal{G}_{1,n,2}$ . Thus  $|(\mathcal{G}_{1,n,2})^c \cap X| = |X|$  is odd and so  $\langle Q_{1,n,2}, \chi(X) \rangle = 1$ . Hence  $Q_{1,n,2} \notin (\bar{C}_{d_n-1})^\perp = F_{d_n-1}$ . ■

We now put forward our *main conjecture*. See section 3.3 for some evidence in its support.

**Conjecture 3.3** *For all  $n \geq 3$  the Grassmannian  $\mathcal{G}_{1,n,2}$  has polynomial degree  $d_n = \binom{n}{2} - 1$ . That is, if  $Q_{1,n,2} := \chi((\mathcal{G}_{1,n,2})^c)$  then  $Q_{1,n,2} \in F_{d_n} \setminus F_{d_n-1}$ . Equivalently, by equation (3.4),  $Q_{1,n,2} \in C_n \setminus C_{n+1}$ .*

We hasten to add that the  $\text{GF}(q)$  version of the result (3.5) was obtained and used by Glynn, Maks & Casse in [4], and that our conjecture 3.3 is just the  $q = 2$  special case of a  $\mathcal{G}_{1,n,q}$  conjecture in [4]. However, for  $n > 3$  no evidence is provided in [4] for the more general conjecture, and even in the special case  $q = 2$  the only evidence given is our own result for  $\mathcal{G}_{1,4,2}$  in [11].

### 3.2 Testing the main conjecture

In the next theorem we consider the application of conditions C.1 - C.6 of theorem 2.1 to our present  $\mathcal{G}_{1,n,2}$  concerns. For the application of condition C.4, let  $\Omega(i), i = 1, 2, \dots$  denote the  $\text{GL}(n+1, 2)$ -orbits of  $d_n$ -flats of  $\text{PG}(N, 2)$ , and let  $X(i)$  be a representative of  $\Omega(i)$ .

For the application of conditions C.5 and C.6 it helps if we make use of certain (simple) graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  having vertex set  $\mathcal{V}_n := \{1, 2, \dots, n+1\}$  and edge set  $\mathcal{E}$ . Along with  $\Gamma$  we will also need its complement  $\bar{\Gamma} = (\mathcal{V}_n, \bar{\mathcal{E}})$ . In section 1 a point  $x \in S = \text{PG}^{(0)}(N, 2)$  had coordinates  $(x_1, x_2, \dots, x_{N+1})$  relative to a choice of basis  $\{e_1, e_2, \dots, e_{N+1}\}$  for  $V_{N+1}$ . In our present area of concern a basis  $\{e_1, e_2, \dots, e_{n+1}\}$  for  $V_{n+1}$  gives rise to a product basis  $\{e_i \wedge e_j\}_{1 \leq i < j \leq n+1}$  for  $V_{N+1} = \wedge^2 V_{n+1}$ , and a point  $x = \sum_{1 \leq i < j \leq n+1} x_{ij} e_i \wedge e_j \in S$  has coordinates  $(x_{ij})_{1 \leq i < j \leq n+1}$ . To each edge  $E = ij := \{i, j\} \in \mathcal{E}$  of

a (simple) graph  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  let us associate

- (i) the coordinate  $x_E := x_{ij}(= x_{ji})$ , and hence the hyperplane  $x_E = 0$ ;
- (ii) the basis element  $e_E := e_i \wedge e_j$  for  $V_{N+1}$ .

Given a graph  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  let  $X_{\mathcal{E}}$  denote the flat having coordinate equations  $x_E = 0$ , each  $E \in \mathcal{E}$ , and set  $Y(\mathcal{E}) := \langle \{e_E \mid E \in \mathcal{E}\} \rangle$ . Then, cf. eq. (1.17),  $x \in Y(\bar{\mathcal{E}})$  if and only if  $x = \sum_{E \in \bar{\mathcal{E}}} x_E e_E$ , that is if and only if  $x_E = 0$ , for each  $E \in \mathcal{E}$ . Hence we have result (i) of:

$$(i) X_{\mathcal{E}} = Y(\bar{\mathcal{E}}); \quad (ii) \chi((X_{\mathcal{E}})^c) = 1 + \prod_{E \in \mathcal{E}} (1 + x_E), \quad (3.6)$$

with the result (ii) being an instance of the result in lemma 1.3. Observe that if  $|\mathcal{E}| = n$ , then  $|\bar{\mathcal{E}}| = \binom{n+1}{2} - n = d_n + 1$ , whence  $Y(\bar{\mathcal{E}})$  is a  $d_n$ -flat.

For the application of condition C.6, note that all graphs  $(\mathcal{V}_n, \mathcal{E})$  of an isomorphism class are generated by that subgroup  $G_0 \cong \text{Sym}(n+1)$  of  $\text{GL}(n+1, 2)$  which effects all permutations of the basis  $\{e_1, e_2, \dots, e_{n+1}\}$ . If  $\gamma(i)$ ,  $i = 1, 2, \dots$  denote the distinct isomorphism classes of simple graphs  $(\mathcal{V}_n, \mathcal{E})$  having  $|\mathcal{E}| = n$  edges, let  $(\mathcal{V}_n, \mathcal{E}(i))$  be a representative of  $\gamma(i)$ .

**Theorem 3.4** *Conjecture 3.3 will hold provided that any one of the following propositions is true:*

P.1. *there exist a family  $\Psi$  of  $n$ -flats of  $\text{PG}(N, 2)$  such that*

$$Q_{1,n,2} = \sum_{X \in \Psi} \chi(X^c); \quad (3.7)$$

P.2. *every  $d_n$ -flat of  $\text{PG}(N, 2)$  meets  $\mathcal{G}_{1,n,2}$  in an odd number of points;*

P.3. *there exists a family  $\Psi$  of  $d_n$ -flats of  $\text{PG}(N, 2)$  such that (i) each  $X \in \Psi$  meets  $\mathcal{G}_{1,n,2}$  in an odd number of points, and (ii)  $\prec \{\chi(X^c)\}_{X \in \Psi} \succ = C_{d_n}$ ;*

P.4. *each of the  $d_n$ -flats  $X(i)$ ,  $i = 1, 2, \dots$  has odd intersection with  $\mathcal{G}_{1,n,2}$ ;*

P.5. *for each graph  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  of size  $|\mathcal{E}| = n$  the  $d_n$ -flat  $Y(\bar{\mathcal{E}})$  has odd intersection with  $\mathcal{G}_{1,n,2}$ ;*

P.6. *each of the  $d_n$ -flats  $Y(\bar{\mathcal{E}(i)})$ ,  $i = 1, 2, \dots$  has odd intersection with  $\mathcal{G}_{1,n,2}$ .*

**Proof.** Conditions C.1 - C.6 of theorem 2.1 are seen to translate into conditions P.1 - P.6 of the present theorem. (In translating conditions C.5 and C.6, note from theorem 3.1 that  $Q_{1,n,2} \in F_{d_n+1}$ .) Hence from theorem 2.1 it follows that any one of conditions P.1 - P.6 suffices to prove that  $Q_{1,n,2} \in F_{d_n}$ . But it then follows from theorem 3.2 that  $\mathcal{G}_{1,n,2}$  has polynomial degree  $d_n$ . ■

### 3.3 In support of the main conjecture

In this section, by appeal to P.6 of theorem 3.4, we demonstrate that conjecture 3.3 holds in the cases  $n \leq 7$ .

**Theorem 3.5** *For  $3 \leq n \leq 7$  the polynomial degree of  $\mathcal{G}_{1,n,2}$  is  $d_n = \binom{n}{2} - 1$ .*

To prove the theorem we will appeal to P.6 of theorem 3.4, tackling the cases  $n = 3, 4, 5, 6, 7$  in turn. Note that for small values of  $n$  the values of  $N (= N_n)$  and  $d_n$  are as in the table:

$n$	$\mathcal{G}_{1,n,2} \subset \text{PG}(N, 2)$	$N = \binom{n+1}{2} - 1$	$d_n = \binom{n}{2} - 1$
3	$\mathcal{G}_{1,3,2} \subset \text{PG}(5, 2)$	5	2
4	$\mathcal{G}_{1,4,2} \subset \text{PG}(9, 2)$	9	5
5	$\mathcal{G}_{1,5,2} \subset \text{PG}(14, 2)$	14	9
6	$\mathcal{G}_{1,6,2} \subset \text{PG}(20, 2)$	20	14
7	$\mathcal{G}_{1,7,2} \subset \text{PG}(27, 2)$	27	20
8	$\mathcal{G}_{1,8,2} \subset \text{PG}(35, 2)$	35	27

### 3.3.1 The Grassmannian $\mathcal{G}_{1,3,2} \subset \text{PG}(5, 2)$

Here  $n = 3$ ,  $N_n = 5$  and  $d_n = 2$ . Up to isomorphism there are precisely three graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  on  $|\mathcal{V}_n| = n + 1 = 4$  vertices having  $|\mathcal{E}| = n = 3$  edges. The edge sets  $\bar{\mathcal{E}}_1, \bar{\mathcal{E}}_2, \bar{\mathcal{E}}_3$  of the complements of these graphs accordingly may be taken to be

$$\bar{\mathcal{E}}_1 = \{12, 13, 14\}, \quad \bar{\mathcal{E}}_2 = \{12, 13, 23\}, \quad \bar{\mathcal{E}}_3 = \{12, 23, 34\}. \quad (3.8)$$

Hence  $Y(\bar{\mathcal{E}}_1) = \text{St}(e_1)$ ,  $Y(\bar{\mathcal{E}}_2) = P(\langle e_1, e_2, e_3 \rangle)$  and  $Y(\bar{\mathcal{E}}_3) = \langle e_1 \wedge e_2, e_2 \wedge e_3, e_3 \wedge e_4 \rangle$ . Consequently  $|\mathcal{G}_{1,3,2} \cap Y(\bar{\mathcal{E}}_i)| = 7, 7, 5$  according as  $i = 1, 2, 3$ . So P.6 of theorem 3.4 holds, and we deduce:

*The Grassmannian  $\mathcal{G}_{1,3,2}$  has polynomial degree  $d_3 = 2$ .*

Of course this is hardly breaking news, since  $\mathcal{G}_{1,3,2}$  is the Klein quadric!

### 3.3.2 The Grassmannian $\mathcal{G}_{1,4,2} \subset \text{PG}(9, 2)$

Here  $n = 4$ ,  $N_n = 9$  and  $d_n = 5$ . Up to isomorphism there are precisely six graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  on  $|\mathcal{V}_n| = n + 1 = 5$  vertices having  $|\mathcal{E}| = n = 4$  edges. The edge sets  $\bar{\mathcal{E}}_i$ ,  $i = 1, 2, \dots, 6$  of the complements of these graphs may be taken to be

$$\begin{aligned} \bar{\mathcal{E}}_1 &= \{12, 13, 14, 23, 24, 34\}; & \bar{\mathcal{E}}_2 &= \{12, 13, 14, 15, 23, 24\}; & \bar{\mathcal{E}}_3 &= \{12, 13, 15, 23, 24, 34\}; \\ \bar{\mathcal{E}}_4 &= \{12, 13, 14, 15, 23, 45\}; & \bar{\mathcal{E}}_5 &= \{12, 13, 14, 23, 25, 45\}; & \bar{\mathcal{E}}_6 &= \{13, 14, 15, 23, 24, 25\}. \end{aligned} \quad (3.9)$$

The intersections of the six 5-flats  $Y(\bar{\mathcal{E}}_i)$  with  $\mathcal{G}_{1,4,2}$  are easily determined:

5-flat	$Y(\bar{\mathcal{E}}_1)$	$Y(\bar{\mathcal{E}}_2)$	$Y(\bar{\mathcal{E}}_3)$	$Y(\bar{\mathcal{E}}_4)$	$Y(\bar{\mathcal{E}}_5)$	$Y(\bar{\mathcal{E}}_6)$
$ \mathcal{G}_{1,4,2} \cap Y(\bar{\mathcal{E}}_i) $	35	27	23	23	19	21

(The first entry is immediate, since  $Y(\bar{\mathcal{E}}_1) = \mathbb{P}(\wedge^2 V_4)$ ,  $V_4 = \langle e_1, e_2, e_3, e_4 \rangle$ .) So P.6 of theorem 3.4 holds, and we deduce:

*The Grassmannian  $\mathcal{G}_{1,4,2}$  has polynomial degree  $d_4 = 5$ .*

This is in agreement with the result obtained in [11]. While our present geometric approach yields  $d_4 = 5$  more quickly, the algebraic computation in [11] found the explicit form, see equation (4.3), of the quintic polynomial function  $Q_{1,4,2} = \chi((\mathcal{G}_{1,4,2})^c)$ .

### 3.3.3 The Grassmannian $\mathcal{G}_{1,5,2} \subset \text{PG}(14, 2)$

Here  $n = 5$ ,  $N_n = 14$  and  $d_n = 9$ . Up to isomorphism there are precisely 15 graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  on  $|\mathcal{V}_n| = n + 1 = 6$  vertices having  $|\mathcal{E}| = n = 5$  edges. The edge sets  $\mathcal{E}_i$ ,  $i = 1, 2, \dots, 15$ , of these graphs may be taken to be

$$\begin{aligned} \mathcal{E}_1 &= \{65, 64, 63, 54, 53\}; & \mathcal{E}_2 &= \{65, 64, 63, 62, 54\}; & \mathcal{E}_3 &= \{65, 64, 62, 54, 53\}; \\ \mathcal{E}_4 &= \{65, 64, 63, 53, 42\}; & \mathcal{E}_5 &= \{64, 63, 62, 54, 53\}; & \mathcal{E}_6 &= \{64, 63, 53, 52, 42\}; \\ \mathcal{E}_7 &= \{65, 64, 63, 62, 61\}; & \mathcal{E}_8 &= \{65, 63, 62, 61, 54\}; & \mathcal{E}_9 &= \{65, 63, 62, 54, 51\}; \\ \mathcal{E}_{10} &= \{65, 64, 63, 54, 21\}; & \mathcal{E}_{11} &= \{65, 64, 61, 52, 43\}; & \mathcal{E}_{12} &= \{64, 63, 61, 54, 52\}; \\ \mathcal{E}_{13} &= \{64, 63, 52, 51, 43\}; & \mathcal{E}_{14} &= \{65, 63, 54, 43, 21\}; & \mathcal{E}_{15} &= \{64, 63, 53, 52, 41\}. \end{aligned} \tag{3.10}$$

While the task of determining by hand the intersections of the fifteen 9-flats  $Y(\bar{\mathcal{E}}_i)$  with  $\mathcal{G}_{1,5,2}$  is straightforward, nevertheless it is a very tedious one, and consequently error-prone. So we resorted to the computer to determine all of the  $|\mathcal{G}_{1,5,2} \cap Y(\bar{\mathcal{E}}_i)|$ , contenting ourselves to checking the results in only a handful of cases. (One easy case is  $i = 7$ , since  $Y(\bar{\mathcal{E}}_7) = \mathbb{P}(\wedge^2 V_5)$ , for  $V_5 = \prec e_1, e_2, e_3, e_4, e_5 \succ$ , and so  $|\mathcal{G}_{1,5,2} \cap Y(\bar{\mathcal{E}}_7)| = |\mathcal{G}_{1,4,2}| = 155$ . In the case  $i = 6$ , one can take advantage of the  $Z_5$ -symmetry  $\langle\langle 23456 \rangle\rangle$  to reduce the length of the computation, and to find  $|\mathcal{G}_{1,5,2} \cap Y(\bar{\mathcal{E}}_6)| = 71$ .) The results found for  $y_i := |\mathcal{G}_{1,5,2} \cap Y(\bar{\mathcal{E}}_i)|$  are as follows:

$i$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$y_i$	107	107	91	83	83	71	155	99	83	75	71	75	71	65	63

Since all the  $y_i$  are odd, P.6 of theorem 3.4 holds, and we deduce:

*The Grassmannian  $\mathcal{G}_{1,5,2}$  has polynomial degree  $d_5 = 9$ .*

### 3.3.4 The Grassmannian $\mathcal{G}_{1,6,2} \subset \text{PG}(20, 2)$

Here  $n = 6$ ,  $N_n = 20$  and  $d_n = 14$ . Up to isomorphism there are precisely 41 graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  on  $|\mathcal{V}_n| = n + 1 = 7$  vertices having  $|\mathcal{E}| = n = 6$  edges. Again we find by computer that each of the intersections  $\mathcal{G}_{1,6,2} \cap Y(\bar{\mathcal{E}}_i)$  is odd. So P.6 of theorem 3.4 holds, and we deduce:

*The Grassmannian  $\mathcal{G}_{1,6,2}$  has polynomial degree  $d_6 = 14$ .*

### 3.3.5 The Grassmannian $\mathcal{G}_{1,7,2} \subset \text{PG}(27, 2)$

Here  $n = 7$ ,  $N_n = 27$  and  $d_n = 20$ . Up to isomorphism there are precisely 115 graphs  $\Gamma = (\mathcal{V}_n, \mathcal{E})$  on  $|\mathcal{V}_n| = n + 1 = 8$  vertices having  $|\mathcal{E}| = n = 7$

edges. Again we find by computer that each of the intersections  $\mathcal{G}_{1,7,2} \cap Y(\bar{\mathcal{E}}_i)$  is odd. So P.6 of theorem 3.4 holds, and we deduce:

*The Grassmannian  $\mathcal{G}_{1,7,2}$  has polynomial degree  $d_7 = 20$ .*

**Remark 3.6** *Viewing the points of  $\mathbb{P}(\wedge^2 V_{n+1}) = \text{PG}(N, 2)$  as alternating matrices of size  $n + 1$ , we used Magma [2] to compute the ranks of all the elements of the  $d_n$ -flats  $Y(\bar{\mathcal{E}}_i)$ . For example, in the  $n = 7$  case, for one of the 115 edge sets  $\mathcal{E}$  we found that of the  $2^{21} - 1 = 2,097,151$  points of the 20-flat  $Y(\bar{\mathcal{E}})$  there were 747, 84, 308, 1, 233, 856 and 778, 240 which had rank 2, 4, 6 and 8, respectively. Of course for our present purposes we did not need all this information! All we needed was that the intersection  $\mathcal{G}_{1,7,2} \cap Y(\bar{\mathcal{E}}_i)$  comprised an odd number, 747, of points.*

## 4 Other approaches

### 4.1 Algebraic approach: use of the Grassmann relations

In this section we consider the algebraic determination of the polynomial degree of a Grassmannian  $\mathcal{G}_{1,n,2}$ , by making use of the well-known quadratic Grassmann conditions and appealing to equation (2.2). First of all let us consider the Grassmannian  $\mathcal{G}_{1,4,2} \subset \text{PG}(9, 2)$ . It will help to introduce the following notation. Each solid  $\sigma = \mathbb{P}(V_4)$  in  $\text{PG}(4, 2)$  defines a 5-flat  $\Pi(\sigma) = \mathbb{P}(\wedge^2 V_4)$  in  $\text{PG}(9, 2)$ , and so, upon defining

$$\mathcal{H}(\sigma) = \Pi(\sigma) \cap \mathcal{G}_{1,4,2} \quad \text{and} \quad \mathcal{W}(\sigma) = \Pi(\sigma) \cap \mathcal{G}_{1,4,2}^c, \quad (4.1)$$

the 63 points of  $\Pi(\sigma)$  consist of the 35 points of a hyperbolic quadric  $\mathcal{H}(\sigma)$  (the Grassmannian  $\mathcal{G}_{1,3,2}$  for the lines of the solid  $\sigma$ ) together with the 28 points  $\mathcal{W}(\sigma)$  which are external to  $\mathcal{H}(\sigma)$ . Take note, see [12, Section 1.3], that the thirty-one subsets  $\mathcal{W}(\sigma)$ ,  $\sigma$  a solid in  $\text{PG}(4, 2)$ , yield a partition of the 868 points of  $\mathcal{G}_{1,4,2}^c$  into 31 subsets of size 28.

The Grassmannian  $\mathcal{G}_{1,4,2}$  is in fact usually thought of as the variety in  $\text{PG}(9, 2)$  determined by the simultaneous solutions of five quadratic conditions  $g_{ijkl}(x) = 0$ , where

$$g_{ijkl}(x) := x_{ij}x_{kl} + x_{ik}x_{lj} + x_{il}x_{jk}, \quad \text{with } \{i, j, k, l\} \subset \{1, 2, 3, 4, 5\}. \quad (4.2)$$

Here the  $x_{ij}(= x_{ji})$  are the coordinates of the bivector  $x \in V_{10}$  with respect to a product basis  $\{e_i \wedge e_j\}_{1 \leq i < j \leq 5}$ . If  $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$  then the set of points  $\psi_{ijkl}$  satisfying  $g_{ijkl}(x) = 0$  is a quadratic cone  $\Pi_3 \mathcal{H}$ , see [6], whose vertex  $\Pi_3$  is the 3-flat  $\text{St}(e_m)$ , and which has as a base the Grassmannian (Klein quadric)  $\mathcal{H} = \mathcal{H}(\sigma_{ijkl}) \subset \Pi(\sigma_{ijkl})$  for the 35 lines of the solid  $\sigma_{ijkl} := \langle e_i, e_j, e_k, e_l \rangle$ . It is easy to see that

$$\psi_{ijkl}(= \text{St}(e_m) \mathcal{H}(\sigma_{ijkl})) = \mathcal{G}_{1,4,2} \cup_{\sigma \ni e_m} \mathcal{W}(\sigma).$$

Now no solid  $\sigma$  in  $\text{PG}(4, 2)$  contains all five points  $e_m, m = 1, 2, 3, 4, 5$ . Consequently the intersection of all five cones  $\psi_{ijkl}$  is indeed  $\mathcal{G}_{1,4,2}$ .

From the five relations (4.2) we can, by using (2.2), determine  $Q_{1,4,2} = \chi((\mathcal{G}_{1,4,2})^c)$ . This algebraic computation was carried out in [11], where it was found that  $Q_{1,4,2}$  was the following explicit quintic polynomial:

$$\begin{aligned} Q(x) &= Q_2(x) + Q_3(x) + Q_4(x) + Q_5(x), \text{ where} \\ Q_2(x) &= \Sigma x_{ij}x_{kl} \quad (15 \text{ terms}), \\ Q_3(x) &= \Sigma x_{ij}x_{jk}x_{lm} \quad (30 \text{ terms}), \\ Q_4(x) &= \Sigma x_{ij}x_{jk}x_{ki}x_{lm} \quad (10 \text{ terms}), \\ Q_5(x) &= \Sigma x_{ij}x_{jk}x_{kl}x_{lm}x_{mi} \quad (12 \text{ terms}). \end{aligned} \quad (4.3)$$

In the case of the Grassmannian  $\mathcal{G}_{1,5,2} \subset \text{PG}(14, 2)$  there are fifteen Grassmann relations  $\psi_{ijkl} = 0$ , one for each 4-subset  $\{i, j, k, l\}$  of  $\{1, 2, 3, 4, 5, 6\}$ . Now we may use (2.2) to find  $Q_{1,5,2}$ , but, before simplification and reduction of degree, there are over  $10^9$  terms to consider. It therefore seemed that computer assistance was required. By computer we found the explicit polynomial  $Q_{1,5,2}$  to be of degree 9, in agreement with conjecture 3.3.

However for much larger values of  $n$  it would seem that computer use of this algebraic approach would not be feasible. Thus for  $\mathcal{G}_{1,7,2}$  there are  $\binom{8}{4} = 70$  Grassmann conditions, and so, before simplification and reduction of degree, the r.h.s. of (2.2) contains more than  $10^{42}$  terms.

**Remark 4.1** *Incidentally, by computer, we did succeed in using the Grassmann relations to obtain one  $q > 2$  result. Namely we were able to show that  $\mathcal{G}_{1,4,3}$  has polynomial degree 10. So there is at least this one piece of evidence for the general  $\text{GF}(q)$  conjecture put forward in [4].*

#### 4.1.1 A more detailed main conjecture

The algebraic approach, when it can be carried out, at least has the advantage of providing more information than the geometric approach, in that it yields the explicit polynomial  $Q_{1,n,2}$ , and not just the degree. By examining the explicit polynomial  $Q_{1,n,2}$  in the cases  $n = 3, 4, 5$ , we were led to put forward a more detailed version of our main conjecture, which we now describe.

With respect to a basis  $\{e_1, e_2, \dots, e_{n+1}\}$  for  $V_{n+1}$  consider the family  $\Psi = \{Y_{i_1 i_2 \dots i_n}\}$  of  $n$ -flats in  $\text{PG}(N, 2)$ , where  $(i_1 i_2 \dots i_n)$  is a cyclic permutation of  $\{1, 2, \dots, n+1\}$  and where

$$Y_{i_1 i_2 \dots i_n} = \langle e_1 \wedge e_{i_1}, e_{i_1} \wedge e_{i_2}, \dots, e_{i_n} \wedge e_1 \rangle. \quad (4.4)$$

Since  $Y_{i_1 i_2 \dots i_n} = Y_{i_n \dots i_2 i_1}$ , observe that  $|\Psi| = \frac{1}{2}n!$ . (So for  $n = 3, 4, 5, 6, \dots$   $|\Psi| = 3, 12, 60, 360, \dots$ ) Consider the function  $f$  defined by

$$f = \sum_{Y \in \Psi} \chi(Y^c). \quad (4.5)$$

Note therefore that  $f$  is an element of  $C_n = F_{d_n}$ , and has polynomial degree  $d_n$ . In the notation of section 3.2 observe that  $f = \sum_{\mathcal{E}} \chi(Y(\mathcal{E})^c)$ , where the summation is over those edge-sets  $\mathcal{E}$  of size  $n + 1$  which constitute an  $(n + 1)$ -cycle.

**Conjecture 4.2**  $Q_{1,n,2} = f + (\text{terms of degree } < d_n)$ .

In support of this conjecture consider first the  $n = 3$  case, where the three 3-flats (i)  $Y_{234}$ , (ii)  $Y_{243}$ , (iii)  $Y_{324}$  have equations (i)  $x_{13} = x_{24} = 0$ , (ii)  $x_{14} = x_{23} = 0$ , (iii)  $x_{12} = x_{34} = 0$ , respectively. So, by equation (1.14),

$$f = x_{13}x_{24} + x_{14}x_{23} + x_{12}x_{34} + (\text{terms of degree } \leq 1).$$

Hence conjecture 4.2 holds true for  $n = 3$ , since  $Q_{1,3,2} = x_{13}x_{24} + x_{14}x_{23} + x_{12}x_{34}$ . It follows from equation (4.3) that the conjecture holds up also when  $n = 4$ . Moreover, using the computer calculation of the explicit polynomial  $Q_{1,5,2}$  of degree 9 referred to above, we find that the more detailed conjecture holds up also if  $n = 5$ .

**Remark 4.3** For  $n > 3$  the polynomial  $f$  in (4.5) can equally well be expressed  $f = \sum_{Y \in \Psi} \chi(Y)$ . This is so since  $|\Psi| (= \frac{1}{2}n!)$  is even for  $n > 3$ .

## 4.2 Further appeals to theorem 3.4

In section 3.3 we obtained some results by appeal to P.6 of theorem 3.4. In this section we consider tackling the general conjecture by appealing instead to P.1, or to P.4, or to P.3.

### 4.2.1 Geometric canonical forms

Since we are working over  $\text{GF}(2)$ , for any subsets  $\psi, \psi_1, \psi_2$  of  $S$  we have

$$\psi = \psi_1 \triangle \psi_2 \iff \chi_\psi = \chi_{\psi_1} + \chi_{\psi_2}, \quad (4.6)$$

where  $\triangle$  denotes the symmetric difference of sets. Consequently equation (3.7) in P.1 of theorem 3.4 is equivalent to

$$(\mathcal{G}_{1,n,2})^c = \triangle_{X \in \Psi} X^c. \quad (4.7)$$

In general if a subset  $\psi$  of  $\text{PG}^{(0)}(N, 2)$  has a reasonably simple expression as a symmetric difference of projective flats, we think of this as a *geometric canonical form* for  $\psi$ . For example, as an illustration of  $F_2 = C_3$  in the case  $N = 5$ , a non-singular elliptic quadric  $\psi$  in  $\text{PG}(5, 2)$  possesses the geometric canonical form  $\psi = X_1 \triangle X_2 \triangle X_3$  (and hence  $\psi^c = X_1^c \triangle X_2^c \triangle X_3^c$ ) where  $X_1, X_2, X_3$  are any three 3-flats in ‘general position’ in  $\text{PG}(5, 2)$ . It seems to us to be an attractive feature of such geometric canonical forms that

they usually have a coordinate-free description, and that certain geometric properties of  $\psi$  may well be arrived at as simple consequences. For example, from  $\psi = X_1 \triangle X_2 \triangle X_3$  one quickly sees that the elliptic quadric  $\psi$  possesses a spread of 9 lines.

Nevertheless we have to confess to having little success in finding a requisite family  $\Psi$  for  $(\mathcal{G}_{1,n,2})^c$  in (4.7). Except that is in the baby case  $n = 3$ , where we have  $(\mathcal{G}_{1,3,2})^c = X_1^c \triangle X_2^c \triangle X_3^c \triangle H^c (= X_1 \triangle X_2 \triangle X_3 \triangle H)$ , for appropriate 3-flats  $X_i$  and 4-flat  $H$ . (Here of course  $H$  can be expressed, in many ways, as the symmetric difference of three 3-flats. Consequently (4.7) holds in the case  $n = 3$ , one possibility having  $|\Psi| = 6$ . In the cases  $n > 3$  several promising choices for  $\Psi$  failed, and all that we can say is that we came to the tentative conclusion that  $\Psi$  could not be a  $\text{GL}(n+1, 2)$ -orbit of  $n$ -flats — in contrast with the  $\text{GL}(n+1, 2)$ -orbit of Latin  $(n-1)$ -flats successfully used in equation (3.5) to prove theorem 3.1. (See however section 4.1.1: if conjecture 4.2 holds up, then the terms of degree  $d_n$  in  $Q_{1,n,2}$  involve a  $G_0$ -orbit of  $n$ -flats, where  $G_0 \cong \text{Sym}(n+1)$  is that subgroup of  $\text{GL}(n+1, 2)$  which stabilizes the basis for  $V_{n+1}$ .)

#### 4.2.2 $\text{GL}(n+1, 2)$ -orbits of $d_n$ -flats

In order to apply P.4 of theorem 3.4, we need to know the  $\text{GL}(n+1, 2)$ -orbits  $\Omega(i), i = 1, 2, \dots$ , of  $d_n$ -flats of  $\text{PG}(N, 2)$ . In the baby case  $n = 3, d_n = 2$ , it is not difficult to see that the 1395 planes in  $\text{PG}(5, 2)$  fall into the following six  $\text{GL}(4, 2)$ -orbits

- $\Omega(1)$  : 15 Latin planes, internal to  $\mathcal{G}_{1,3,2}$ ;
- $\Omega(2)$  : 15 Greek planes, internal to  $\mathcal{G}_{1,3,2}$ ;
- $\Omega(3)$  : 630 planes, meeting  $\mathcal{G}_{1,3,2}$  in a pair of intersecting lines;
- $\Omega(4)$  : 105 planes, each meeting  $\mathcal{G}_{1,3,2}$  in a line;
- $\Omega(5)$  : 560 planes, each meeting  $\mathcal{G}_{1,3,2}$  in a conic;
- $\Omega(6)$  : 70 planes, each meeting  $\mathcal{G}_{1,3,2}$  in a single point.

So P.4 holds in this case, confirming that  $\mathcal{G}_{1,3,2}$  has polynomial degree 2.

Consider next the case of  $\mathcal{G}_{1,4,2}$ . Now in [12] much effort was expended to classify just one kind of flat in  $\text{PG}(9, 2)$ , namely those external to  $\mathcal{G}_{1,4,2}$ . Possibly this work could be built upon to determine the  $\text{GL}(5, 2)$ -orbits of all of the 53,743,987 5-flats in  $\text{PG}(9, 2)$ , but it would appear to be a daunting task. *Certainly for  $n > 4$  it does not at all seem feasible to attempt to apply P.4 of theorem 3.4.*

#### 4.2.3 $\text{GL}(n+1, 2)$ -orbits which span $C_{d_n}$ ?

As  $n$  increases the number of  $\text{GL}(n+1, 2)$ -orbits increases inordinately. So, following on from the pessimistic ending of the preceding section, it seems to us that if we wish to prove the main conjecture, and not merely produce hard-won evidence for it in particular cases, the best hope is that, for each

$n$ , there exists one kind of  $\text{GL}(n+1, 2)$ -orbit  $\Omega_n$  of  $d_n$ -flats of  $\text{PG}(N, 2)$  such that the functions  $\chi(X^c)$ ,  $X \in \Omega_n$ , span the whole of  $F_n = C_{d_n}$ . (We should perhaps stress that we are dealing here with  $\text{GL}(n+1, 2)$ -orbits, not  $\text{GL}(N+1, 2)$ -orbits! For note, by the composition series (1.20) for  $F(S)$  in theorem 1.9, that *any*  $\text{GL}(N+1, 2)$ -orbit generated by an element of  $F_r \setminus F_{r-1}$  spans the whole of  $F_r$ .) For if, for each  $n$ , such an orbit  $\Omega_n$  can be found, and if for just one flat  $X \in \Omega_n$  we can show that  $X$  meets  $\mathcal{G}_{1,n,2}$  in an odd number of points, then it would follow, *cf.* P.3 of theorem 3.4, that the polynomial degree of  $\mathcal{G}_{1,n,2}$  is  $d_n$ . (Of course if for a particular  $n$  we found that the flats  $X \in \Omega_n$  meet  $\mathcal{G}_{1,n,2}$  in an even number of points, then the main conjecture would be refuted, and for this particular  $n$  the polynomial degree of  $\mathcal{G}_{1,n,2}$  would be  $d_n + 1$ .)

*Acknowledgement.* While amassing in section 3.3 evidence in support of the main conjecture, we were (in the cases  $n = 6$  and  $n = 7$ ) greatly indebted to L.H. Soicher, who provided us with lists of edge sets for the different kinds of simple graphs of order  $n+1$  and size  $n$ ,  $n \leq 8$ . He generated these lists by treating simple graphs as simple binary block designs with blocks of size 2, and using his recently released DESIGN Package for GAP, see [13].

## References

- [1] E.F. Assmus and J.D. Key, Designs and their Codes, Cambridge University Press, Cambridge (1993).
- [2] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, J. Symbol. Comput., 24 (1997), 235-265.
- [3] B.N. Cooperstein, External flats to varieties in  $\text{PG}(\Lambda^2 V)$  over finite fields. Geom. Dedicata 69 (1998), 223-235.
- [4] David G. Glynn, Johannes G. Maks, L.R.A. (Rey) Casse, The polynomial degree of the Grassmannian  $\mathcal{G}(n, 1, q)$  of lines in finite projective space  $\text{PG}(n, q)$ , preprint (July 2003).
- [5] N.A. Gordon, T.M. Jarvis, J.G. Maks and R. Shaw, Composition algebras and  $\text{PG}(m, 2)$ , J. Geom. 51, (1994), 50-59.
- [6] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions Clarendon, Oxford, 1985.
- [7] J.W.P. Hirschfeld and R. Shaw, Projective geometry codes over prime fields, see AMS Contemporary Mathematics Series, Vol. 168, Finite Fields: Theory, Applications and Algorithms, eds. G. Mullen & P. J.-S. Shiue, Amer. Math. Soc. (1994), pp.151-163.

- [8] R. Shaw, A characterization of the primals in  $\text{PG}(m, 2)$ , *Designs, Codes and Crypt.* 2 (1992), 253-256.
- [9] R. Shaw, Finite geometries and Clifford algebras III, see *Proc. of the 2nd Workshop on Clifford Algebras and their Applications in Mathematical Physics*, Montpellier, France, (1989); eds. A. Micali et al., *Kluwer Acad. Pubs.* (1992), pp. 121-132.
- [10] R. Shaw, Composition algebras,  $\text{PG}(m, 2)$  and non-split group extensions, see *Proc. of XIXth International Colloquium on Group Theoretical Methods in Physics*, Salamanca (1992), eds. M. A. del Olmo et al., *Anales de Fisica, Monografias*, Vol. 1, CIEMAT/RSEF, Madrid (1993), pp. 467-470.
- [11] R. Shaw and N.A. Gordon, The lines of  $\text{PG}(4, 2)$  are the points of a quintic in  $\text{PG}(9, 2)$ , *J. Combin. Theory (A)*, 68 (1994), 226-231.
- [12] R. Shaw, J.G. Maks and N.A. Gordon, The classification of flats in  $\text{PG}(9, 2)$  which are external to the Grassmannian  $\mathcal{G}_{1,4,2}$ , *Des. Codes Cryptogr.*, 34 (2005) 203-227.
- [13] L.H. Soicher, The Design Package for GAP,  
[http://designtheory.org/software/gap\\_design/](http://designtheory.org/software/gap_design/) .