The Binary Self-Dual Codes of Length Up To 32: A Revised Enumeration*

J. H. Conway

Mathematics Department
Princeton University
Princeton, New Jersey 08540

*V. Pless***

Mathematics Department
University of Illinois at Chicago
Chicago, Illinois 60680

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

February 28, 1990

* This paper appeared in *J. Combinatorial Theory*, *Series A*, **60** (1992), 183-195.

** Research supported in part by Air Force Office of Scientific Research Grant 88027.

1. The 85 doubly-even codes of length 32

In the course of preparing Ref. [4] we discovered certain errors in [10], and this led us to recheck the list of 85 doubly-even self-dual codes of length 32 given in [2]. The actual enumeration of these 85 codes in [2] was subject to many computer checks and was correct, but unfortunately several errors and obscurities have crept into their descriptions as printed in [2]. There are also serious errors in the numbers of children of length 30 (found by hand) for many of these codes. We therefore give (in Table A, at the end of the paper) an amended version of Table III of [2], omitting the glue vectors. The remainder of this section contains comments on this table and further errata to [2].

Names. The 85 codes are given in the same order as in Table III of [2]. We label them $C1, \ldots, C85$ (in the first column of Table A). A star indicates that the code is mentioned in Table C below.

Components. The second column gives the components. Although the component codes d_n, e_n, ... are described in [2], some additional remarks are appropriate.

The code g_{24-m} ($m = 0, 2, 3, 4, 6, 8$) is obtained by taking the words of the extended binary Golay code g_{24} (see [3], [7]) that vanish on m digits (and then deleting those digits). For the [16,5,8] first order Reed-Muller code g_{16} (wrongly called a second order code in [2]) the 8 digits must be a special octad, while for g_{18} they must be an umbral hexad (see [3] or [5] for terminology). For $0 \le m \le 6$, g_{24-m} is a $[24-m,\ 12-m,\ 8]$ code.

The [24,11,8] half Golay code h_{24} consists of the Golay codewords that intersect a given tetrad evenly.

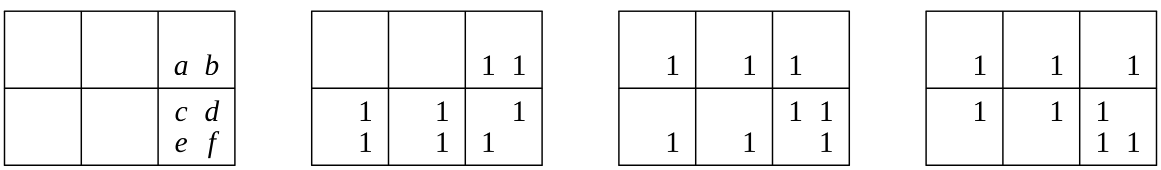
Under the action of $\mathrm{Aut}(g_{24})$ there are two distinct ways to select tetrads $t = \{c, d, e, f\}$, $u = \{a, b, e, f\}$, $v = \{a, b, c, d\}$ so that $t + u + v = 0$, depending on whether $\{a,\ b,\ \ldots,\ f\}$ is a special hexad or an umbral hexad (see Fig. 1). Correspondingly there are two [24,10,8] quarter

Golay codes q_{24}^{+}, q_{24}^{-}, consisting of the codewords of g_{24} that intersect all of t, u, v evenly. In [2] only the second of these was described and was there called q_{24}, while q_{24}^{+} was called $(g_{16} + f_8)$. (The exceptional treatment of the components of this code given on p. 52 of [2] is now eliminated.)

The glue space for either q_{24}^{+} or q_{24}^{-} is four-dimensional, and is generated by t, u, v, p, q, r with

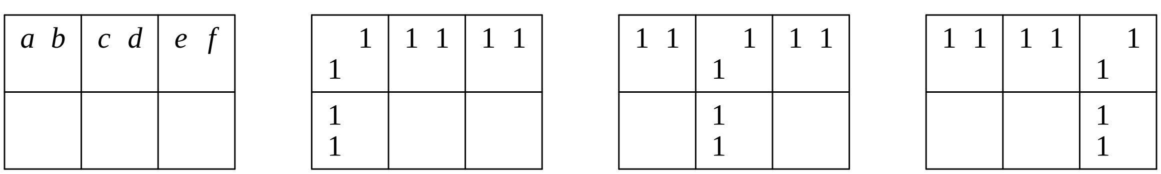
$$t + u + v \ = \ 0 \ = \ p + q + r \ ,$$

where p, q, r may be represented by special octads, with p orthogonal to t but not to u or v, q orthogonal to u but not to t or v, and r orthogonal to v but not to t or u (see Fig. 1).



t, u, v $\qquad$ p $\qquad$ q $\qquad$ r

q_{24}^{+}, $\{a, b, \ldots, f\}$ special



t, u, v $\qquad$ p $\qquad$ q $\qquad$ r

q_{24}^{-}, $\{a, b, \ldots, f\}$ umbral

Fig. 1. The codes q_{24}^{+}, q_{24}^{-}

The 16 glue components and their minimal weights are:

Representative	Minimal Weight
0	0
t, u, v	4
p, q, r	8
$p+u,\ q+v,\ r+t,$ $p+v,\ q+t,\ r+u$	6
$p+t,\ q+u,\ r+v$	8 in q_{24}^{+}, 4 in q_{24}^{-}

The groups. The order $|G|$ of the automorphism group of any of the 85 codes is given (as in [2]) by the formula

$$|G| = |G_0|\ |G_1|\ |G_2|\ ,$$

while $|G_0|$ is the product of the $|G_0|$'s of the component codes, and $|G_1|$, $|G_2|$ are given in the third and fourth columns of Table A. $|G|$ itself is given in the fifth column. Table B gives the groups G_0 (in ATLAS [1] notation) for the components.

Table B
The groups G_0

Component	G_0	$\lvert G_0 \rvert$
d_{2m}	$2^{m-1} . S_m$	$2^{m-1} m!$
e_7	$L_3(2)$	168
e_8	$2^3 . L_3(2)$	1344
f_n	1	1
g_{16}	2^4	16
g_{18}	C_3	3
g_{20}	M_{20}	$2^6 3.5$
g_{21}	M_{21}	$2^6 3^2 5.7$
g_{22}	M_{22}	$2^7 3^2 5.7.11$
g_{24}	M_{24}	$2^{10} 3^3 5.7.11.23$
h_{24}	$2^6 : 3S_6$	$2^9 3^3 5$
q_{24}^{+}	$2^6 . (S_3 \times 2^2)$	$2^9 3$
q_{24}^{-}	$2^2 \times S_4$	$2^5 3$

The mass checks. We repeated various ''mass checks'' on the 85 codes, verifying that the number of codes containing a specified subcode (e.g. d_4 or d_6) is as predicted by the formula given on p. 28 of [2]. In particular we rechecked that the total mass

$$\sum_{(85)} \frac{1}{|G|}$$

of the reciprocals of the numbers in the fifth column of Table A has the correct value

$$\frac{1}{32!} \prod_{i=0}^{14} (2^i + 1) ,$$

which is

$$\frac{391266122896364123}{532283035423762022400} .$$

Weight distributions. The sixth column gives u_4, the number of codewords of weight 4. The full weight distribution can then be obtained from Table IV of [2].

Table C summarizes the amendments to Table III of [2] other than errors in the value of n_{30}.

Table C
Other alterations to Table III of [2]

Code	Components	Change
C22, C39, C53, C65, C70, C71		f_m^2 has been replaced by f_{2m}.
C10	$d_{12}^2 e_8$	$\vert G_2 \vert = 2$, not 1.
C41	$d_8 d_4^4 f_8$	Change *boczxAB* to *boozxAB*.
C61	$d_6 d_4^2 d_4^3 f_3^2$	The final - was omitted.
C66	$d_6 f_{13}^2$	The last character should be - not –
C71	$d_4^6 f_4^2$	The glue generators should be *ooyoxxAE*, *yooxoxBF*, *oyoxxoCD*, *oxyooxCG*, *yoxxooAG*, *xyooxoBG*, *ooxoxyFH*, *xooyoxDH*, *oxoxyoEH*, *oxxooyBD*, *xoxyooCE*, *xxooyoAF*, *ozxozx*-, *xozxoz*-, *xzoxzo*-.
C75	$d_4^4 f_{16}$	The printing of the glue is poorly aligned. Each glue word consists of a top line of 4 letters (chosen from o, x, y, z), with a 4×4 array beneath it.
C77	$d_4^2 q_{24}^+$	Redescribed above.
C78	$d_4^2 q_{24}^-$	Redescribed above.
C79	$d_4^2 f_4^6$	The parentheses around the final array indicate that its six columns are to be bodily permuted.
C80	$d_4 f_7^4$	The third and fourth glue generators should be $y(+++o+oo)(ooooooo)(+oooooo)(+oooooo)$, $y(ooooooo)(+++o+oo)(+oooooo)(+oooooo)$.

Additional errata to [2]

On page 37 the phrase ‘‘Figure (MOG)’’ refers to Ref. [5] (or Fig. 11.17 of [3]).

On p. 44, for the first code in Table I, change e_0 to e_8.

On pp. 46 and 48, the heading should read $n_{30}, n_{28}, n_{26}, n_{24}$ ... .

On p. 52, the last entry in Table V should be 731, not 664.

On p. 53, the last author’s name is misspelled in Ref. [5].

2. Self-dual codes of length less than 32

The numbers of children. We now describe how the final four columns of Table A were obtained. These give n_{30}, n_{28}, n_{26}, n_{24}, the number of self-dual codes (the ‘‘children’’) of lengths $30, \ldots, 24$ that arise from each of the 85 codes.

Any self-dual code C of length 30 is obtained by taking all codewords of one of $C1, \ldots, C85$ for which some particular pair of coordinates P, Q (say) are 00 or 11, and deleting these coordinates. If C contains a weight 2 word, which it does when P and Q belong to a weight 4 word of the original code, we obtain a self-dual code with length less than 30 and $d \geq 4$ by ‘‘collapsing’’ C, i.e. by deleting all pairs of coordinates that support weight 2 words. All self-dual codes with length $n \leq 30$ and $d \geq 4$ can be obtained in this way. There are several cases.

If the coordinates P, Q are in an e_8 the collapsed code is a doubly-even self-dual code of length 24, whose components are obtained by deleting the e_8.

If P, Q are in an e_7 the collapsed code has length 26 and its components are obtained by replacing the e_7 by an f_1.

If P, Q form a duad (a pair of identical coordinates, cf. [2], p. 33) in a d_m, $m \geq 6$, the collapsed code has length $32 - m$ and its components are obtained by deleting the d_m.

If P, Q are in a d_m, $m \geq 6$, but do not form a duad, or if P, Q belong to a d_4 component, the collapsed code has length 28.

In all other cases C does not collapse and we have a self-dual code with length 30 and $d \geq 4$.

As an example we consider the code C61. There are 19 orbits of $\mathrm{Aut}(C61)$ on unordered pairs of distinct coordinates, and so there are $n_{30} = 19$ length 30 children, 6 of which collapse to shorter lengths, as follows. One length 26 child is obtained from a duad in the d_6 (thus $n_{26} = 1$).

From two coordinates in the d_6 not forming a duad we obtain the first child of length 28, while a second child of length 28 is obtained from any two coordinates in the first type of d_4, and three further children of length 28 arise from the three different ways of choosing a pair of coordinates from the other type of d_4. Thus $n_{28} = n_{26} + 5 = 6$. Finally are 13 children with length 30 and $d \geq 4$, so that $n_{30} = n_{28} + 13 = 19$.

In [2] and [10] the actions of the automorphism groups of the 85 codes on pairs of coordinates were found (unfortunately often incorrectly) by hand. In the present version most of this work has been redone by computer (using in particular the graph-automorphism program Nauty [8]). The numbers of children of lengths $n \leq 28$ given in [2] are correct. There are numerous errors in n_{30}, however (now corrected in Table A), and the total number of self-dual codes of length 30 is 731, not 664 as stated in Table V of [2].

Tables of self-dual codes of length n ≤ 24

The self-dual codes of length $n \leq 20$ were first enumerated in [9], and those of lengths 22 and 24 in [11], although there they are not described in the terminology later used in [2]. For completeness we therefore give the components, values of $|G_1|$, $|G_2|$, weight distributions $\{u_i\}$ and glue generators for the codes with $n \leq 22$ in Table D (at the end of the paper). The column headed ‘‘Code’’ gives the parent code of length 32 (with the component to be deleted in parentheses). The column headed ‘‘[9], [11]’’ gives the names used in these papers. ([9], [11] also give generator matrices for these codes.)

Table E lists the codes of length 24, although to save space we just describe each code by giving its parent (and in parentheses the component to be deleted), its components and minimal distance d. If the deleted component (in parentheses) is an e_8 the code is doubly-even, otherwise (if the deleted component is a d_8) it is singly-even.

Table E
Self-dual codes with length 24 and $d \geq 4$

Code	Components	[11]	d	Code	Components	[11]	d
C2(e_8)	d_{24}	E_{24}	4	C32(d_8)	$d_8 e_7^2 f_2$	J_{24}	4
C6(e_8)	$d_{16} e_8$	-	4	C33(d_8)	$d_8 d_6^2 f_4$	R_{24}	4
C7(d_8)	$d_{16} d_8$	H_{24}	4	C34(d_8)	$d_8 d_4^4$	T_{24}	4
C10(e_8)	d_{12}^2	A_{24}	4	C35(d_8)	$e_7 d_6^2 d_4 f_1$	P_{24}	4
C11(d_8)	d_{12}^2	-	4	C26(e_8)	d_6^4	D_{24}	4
C12(d_8)	$d_{12} d_8 d_4$	I_{24}	4	C36(d_8)	d_6^4	Q_{24}	4
C18(e_8)	$d_{10} e_7^2$	B_{24}	4	C37(d_8)	$d_6^2 d_6 d_4 f_2$	S_{24}	4
C19(d_8)	$d_{10} e_7 d_6 f_1$	K_{24}	4	C38(d_8)	$d_6^2 d_4^2 f_4$	U_{24}	4
C20(d_8)	$d_{10} d_6^2 f_2$	N_{24}	4	C39(d_8)	$d_6 d_4^3 f_6$	W_{24}	4
C24(e_8)	e_8^3	-	4	C27(e_8)	d_4^6	F_{24}	4
C25(d_8)	$e_8 d_8^2$	-	4	C40(d_8)	d_4^6	V_{24}	4
C25(e_8)	d_8^3	C_{24}	4	C41(d_8)	$d_4^4 f_8$	X_{24}	4
C29(d_8)	d_8^3	L_{24}	4	C42(d_8)	$d_4^2 g_{16}$	Y_{24}	4
C30(d_8)	d_8^3	M_{24}	4	C43(d_8)	h_{24}	Z_{24}	6
C31(d_8)	$d_8^2 d_4^2$	O_{24}	4	C28(e_8)	g_{24}	G_{24}	8

Codes with d ≥ 6. Similar tables could easily be constructed to list the self-dual codes of lengths 26, 28 and 30, but would occupy too much space. Instead we just describe the 17 codes with $d \geq 6$ (and correct some errors in [10]).

There is one code (A_{26}) of length 26, arising from C66; three codes of length 28, one (A_{28}) from C66 and two (B_{28}, C_{28}) from C80; and thirteen codes ($A_{30}, \ldots, M_{30}$) of length 30, one from each of C77, ..., C82, two from each of C83, C84, and three from C85.

Figure 2 contains generator matrices for C66, C77, ..., C85. Each row of Greek letters below one of these matrices specifies a self-dual child with $d \geq 6$. The child is obtained by restricting to the subcode consisting of the words that are equal on pairs of coordinates described by the same Greek letter, and then deleting these coordinates. (For C83 and C84 we have used the generator matrices described in [6], [12].) The weight distributions are given in Table F (compare [4]).

Table F
Weight distributions of self-dual codes with $n = 26, 28, 30$ and $d \geq 6$

	u_6	u_8	u_{10}	u_{12}	u_{14}
A_{26}	52	390	1313	2340	2340
A_{28}	26	442	1560	3653	5020
$B_{28},\ C_{28}$	42	378	1624	3717	4680
$A_{30},\ B_{30},\ C_{30}$	19	393	1848	5192	8931
D_{30}	27	369	1848	5256	8883
$E_{30}, \ldots, M_{30}$	35	345	1848	5320	8835

Figure 2. Generator matrices for C66, C77, ..., C85 and their children of length 26, 28, 30 and $d = 6$.

C66

```
11110000000000000000000000000000
00111100000000000000000000000000
01010111010000010001000000000000
01010101101000001000100000000000
01010100110100000100010000000000
01010100011010000010001000000000
01010110001101000000000100000000
01010101000110100000000010000000
01010100100011010000000001000000
01010100010001101000000000100000
01010100001000110100000000010000
01010100000100011010000000001000
01010110000010001100000000000100
01010101000001000110000000000010
01010110100000010001000000000001
01011011111111111110000000000000
```

A_{26} ααββγγ

A_{28} αβαβ

C77

```
11110000000000000000000000000000
00001111000000000000000000000000
00000000111111110000000000000000
00000000000000001111111100000000
00000000000000000000000011111111
00000000010101010101010100000000
00000000001100110011001100000000
00000000000011110000111100000000
00000101000001010000010100000101
00000011000000110000001100000011
01010000010100000101000001010000
00110000001100000011000000110000
00000000011110000100010001000100
00000000011110000010001000100010
00000000011110000001000100010001
00000000000000000000111100001111
```

A_{30} α   α

C78

```
11110000000000000000000000000000
00001111000000000000000000000000
00000000101111010110011001010000
00000000100111101011001100101000
00000000100011110101100110010100
00000000100001111010110011001010
00000000110000011110101100110010
00000000010100111010110010101001
00000000111001010000011110101100
00000000001101001110101100101010
00000000111101100010110010001100
00000000111111111111111111111111
01010110100000110010000011100001
01100011010010101100100000001001
01100101000000000000111100000000
00110110000000000000001111000000
```

B_{30} α α

C79

```
11110000000000000000000000000000
00001111000000000000000000000000
00110011001100000000001100000000
00110101000000110000010100000000
00110110000000000011011000000000
01010011010100000000000000110000
01010101000000101000000010100000
01010110000000000101000001100000
01100011011000000000000000000011
01100101000000110000000000000101
00000000011110001000100010001000
00000000100001111000100010001000
00000000100010000111100010001000
00000000100010001000011110001000
00000000100010001000100001111000
00000000100010001000100010000111
```

C_{30} α α

C80

```
11110000000000000000000000000000
01011000000100000010010110000000
01010100000010000011001010000000
01010010000001000011100100000000
01010001000000100011100010000000
01010000100000010010111000000000
01010000010000001001011100000000
01010000001000000100101110000000
01011110100000000010000001000000
01010111010000000001000000100000
01010011101000000000100000010000
01011001110000000000010000001000
01010100111000000000001000000100
01011010011000000000000100000010
01011101001000000000000010000001
00111111111000000011111110000000
```

B_{28} ααββ

C_{28} αβαβ

D_{30} α α

C81

```
10110110111100010101110000100100
10011011011110001010111000010010
10001101101111000101011100001001
11000110110111100010101110000100
10100011011011110001010111000010
10010001101101111000101011100001
11001000110110111100010101110000
10100100011011011110001010111000
10010010001101101111000101011100
10001001000110110111100010101110
10000100100011011011110001010111
11000010010001101101111000101011
11100001001000110110111100010101
11110000100100011011011110001010
10111000010010001101101111000101
11011100001001000110110111100010
```

E_{30} αα

```
              C82
10011100100000100000011000000000
10001110010000010000001100000000
10000111001000001000000110000000
10000011100100000100000011000000
10000001110010000010000001100000
10000000111001000001000000110000
10000000011100100000100000011000
10000000001110010000010000001100
10000000000111001000001000000110
10000000000011100100000100000011
11000000000001110010000010000001
11100000000000111001000001000000
10110000000000011100100000100000
10011000000000001110010000010000
10001100000000000111001000001000
10000110000000000011100100000100
```

F_{30} αα

```
              C83
11101000111010000000000000000000
10110100101101000000000000000000
10011010100110100000000000000000
10001101100011010000000000000000
00000000111010001110100011101000
00000000101101001011010010110100
00000000100110101001101010011010
00000000100011011000110110001101
11011000110110001101100000000000
10101100101011001010110000000000
10010110100101101001011000000000
10001011100010111000101100000000
00000000000000001101100011011000
00000000000000001010110010101100
00000000000000001001011010010110
00000000000000001000101110001011
```

G_{30} αα

H_{30} α α

C84

```
11101000000000001110100011101000
10110100000000001011010010110100
10011010000000001001101010011010
10001101000000001000110110001101
00000000111010001110100010110100
00000000101101001011010010011010
00000000100110101001101010001101
00000000100011011000110111000110
11011000110110001101100000000000
10101100101011001010110000000000
10010110100101101001011000000000
10001011100010111000101100000000
11011000101100010000000011011000
10101100110110000000000010101100
10010110101011000000000010010110
10001011100101100000000010001011
```

I_{30} αα

J_{30} α   α

C85

```
10000000000000001111100010001000
01000000000000001111010001000100
00100000000000001111001000100010
00010000000000001111000100010001
00001000000000001000111110001000
00000100000000001001111010000100
00000010000000001011110010000010
00000001000000001111100010001
00000000100000001000100011111000
00000000010000000100010011110100
00000000001000000010001011110010
00000000000100000001000111110001
00000000000010001000100010001111
00000000000001000100010001001111
00000000000000100010001000101111
00000000000000010001000100011111
```

K_{30} αα

L_{30} α   α

M_{30} α   α

References

1. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, ‘‘ATLAS of Finite Groups’’, Oxford Univ. Press, 1985.

2. J. H. Conway and V. Pless, ‘‘On the enumeration of self-dual codes’’, J. Combinatorial Theory, **A 28** (1980), 26-53.

3. J. H. Conway and N. J. A. Sloane, ‘‘Sphere Packings, Lattices and Groups’’, Springer-Verlag, NY 1988.

4. J. H. Conway and N. J. A. Sloane, ‘‘A new upper bound on the minimal distance of self-dual codes’’, IEEE Trans. Information Theory, submitted.

5. R. T. Curtis, ‘‘A new combinatorial approach to M_{24}’’, Math. Proc. Camb. Phil. Soc., **79** (1976), 25-42.

6. H. V. Koch, ‘‘On self-dual, doubly-even codes of length 32’’, Report P-Math-32/84, Institut für Mathematik, Akademie der Wissenschaften der DDR, Berlin, 1984.

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

8. B. D. McKay, ‘‘NAUTY User’s Guide (Version 1.2)’’, Dept. Computer Science Technical Report TR-CS-87-03, Australian National University, Canberra, Australia, 1987.

9. V. Pless, ‘‘A classification of self-orthogonal codes over $GF(2)$’’, Discrete Math., vol. **3** (1972), pp. 209-246.

10. V. Pless, ‘‘The children of the (32,16) doubly even codes’’, IEEE Trans. Information Theory, **24** (1978), 738-746.

11. V. Pless and N. J. A. Sloane, ‘‘On the classification and enumeration of self-dual codes’’, J. Combinatorial Theory, **A 18** (1975), 313-335.

12. V. Y. Yorgov, ‘‘On the extremal doubly-even codes of length 32’’, Proceedings Fourth Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, 1989, pp. 275-279.

The Binary Self-Dual Codes of Length Up To 32: A Revised Enumeration*

J. H. Conway

Mathematics Department
Princeton University
Princeton, New Jersey 08540

*V. Pless***

Mathematics Department
University of Illinois at Chicago
Chicago, Illinois 60680

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

February 28, 1990

ABSTRACT

This paper presents a revised enumeration of the binary self-dual codes of length up to 32 given in ‘‘On the enumeration of self-dual codes’’ (by J. H. C. and V. P.) and ‘‘The children of the (32,16) doubly even codes’’ (by V. P.). The list of eighty-five doubly-even self-dual codes of length 32 given in the first paper is essentially correct, but several of their descriptions need amending. The principal change is that there are 731 (not 664) inequivalent self-dual codes of length 30. Furthermore there are three (not two) [28,14,6] and thirteen (not eight) [30,15,6] self-dual codes. Some additional information is provided about the self-dual codes of length less than 32.

---

* This paper appeared in *J. Combinatorial Theory, Series A*, **60** (1992), 183-195.

** Research supported in part by Air Force Office of Scientific Research Grant 88027.