Lexicographic Codes: Error-Correcting Codes from Game Theory *

by

J. H. Conway
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
Cambridge, CB2 1SB, England

and

N. J. A. Sloane
Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974, USA

ABSTRACT

Lexicographic codes, or lexicodes, are defined by various versions of the greedy algorithm. The theory of these codes is closely related to the theory of certain impartial games, which leads to a number of surprising properties. For example, lexicodes over an alphabet of size $B = 2^a$ are closed under addition, while if $B = 2^{2^a}$ the lexicodes are closed under multiplication by scalars, where addition and multiplication are in the nim sense explained in the text. Hamming codes and the binary Golay codes are lexicodes. Remarkably simple constructions are given for the Steiner systems S(5, 6, 12) and S(5, 8, 24). Several record-breaking constant weight codes are also constructed.

---

* Appeared in ‘‘IEEE Trans. Information Theory’’, 32 (1986), pp. 337–348.

I. Introduction

This paper is concerned with various classes of *lexicographic codes*, that is, codes that are defined by a greedy algorithm: each successive codeword is selected as the *first* word not prohibitively near (in some prescribed sense) to earlier codewords.

For example, the very simplest class of lexicographic codes is defined as follows. We specify a base B, and a desired minimal Hamming distance d. The first codeword accepted is the zero word. Then we consider all base-B vectors in turn, and accept a vector as a codeword if it is at Hamming distance at least d from all previously accepted codewords. (An example with $B = 3$ and $d = 3$ can be seen in Table XI.)

One of our goals is to point out the essential identity between this kind of lexicographic coding theory and the theory of certain impartial games (see Section II). Then the Sprague-Grundy theory of games has a number of interesting and surprising consequences for lexicographic codes (or *lexicodes*):

(1) Unrestricted binary lexicodes are linear (Theorems 1,3);

(2) For base $B = 2^a$, unrestricted lexicodes are closed under nim-addition (Theorem 4);

(3) For base $B = 2^{2^a}$, unrestricted lexicodes are closed under nim-multiplication, which is an operation that converts the digits $\{0,1,2,3, \ldots, 2^{2^a} - 1\}$ into a field (Theorem 5);

(4) The constant weight binary lexicodes with minimal distance 4 have a rather subtle complete solution in terms of Welter's game (Section (4.3)).

Two other results worth mentioning here are the following.

(5) Several well-known codes unexpectedly turn out to be lexicographic codes, including Hamming codes and the binary Golay codes of length 23 and 24 (Section (3.2)).

(6) The constant weight binary lexicode of length 24, distance 8 and weight 8 is the Steiner system S(5, 8, 24) (Theorem 12). By imposing an additional constraint on a constant weight lexicode (see (4.5)), Ryba obtained an almost equally simple construction for the Steiner system S(5, 6, 12) (Theorem 13). The corresponding game, called Mathematical Blackjack (or Mathieu's Vingt-et-un) is described at the end of Section (4.5).

(7) A number of constant weight codes with minimal distance 10 and containing a record number of codewords are given in Table XIII.

Some of the game-theoretic aspects of this work are described in [1] and [2]. The relations between the theories of games and of lexicographic codes, and in particular the multiplicative theorem, underly some of the results in [1]. However, most of the results are published here for the first time. This work may be regarded as a coding-theoretic analog of the laminated lattices described in [5], [6].

The paper is arranged as follows. The connections with game theory are discussed in Section II, unrestricted lexicodes are treated in Section III, and Section IV deals with constant weight and constrained lexicodes. Tables IV-VII and XII give the parameters of a number of lexicodes.

II. The connections with game theory

(2.1) Grundy's game.

We begin by describing Grundy's game [1, p. 96], [9, p. 8], which is a characteristic example of the class of games to be considered. In Grundy's game the typical position

$$P_a + P_b + P_c + \cdots \qquad (1)$$

consists of a number of heaps containing

$$a, \quad b, \quad c, \quad \cdots$$

objects respectively. There are two players, who move alternately. A legal move is to split any heap into two strictly smaller heaps of distinct sizes, that is, to replace any term P_h in (1) by $P_i + P_j$, where $0 < i < h$, $0 < j < h$, $i \neq j$ and $i + j = h$. The first player who is unable to move loses.

(2.2) Heap games in general

Grundy's game is an example of a *heap game*. The general game of this type may be taken to have certain atomic positions P_i and general position

$$P_a + P_b + P_c + \cdots \; . \qquad (2)$$

The rules are specified by giving an arbitrary family of *turning sets*, a typical turning set being written

$$\{h, i, j, \cdots\} \quad \text{with} \quad h > i > j > \cdots \; .$$

The legal move is to replace any term P_h in (2) by $P_i + P_j + \cdots$, provided that $\{h, i, j, \cdots\}$ is a turning set. For Grundy's game the turning sets are $\{3,2,1\}$,

$\{4,3,1\}, \{5,4,1\}, \{5,3,2\}, \{6,5,1\}$,....

There is a well-known theory of heap games, due to Sprague and Grundy [1], [2], [9], [19]. There is a function $G(P)$ (the *nim-value, Grundy number*, or *G-value*) assigning integer values to positions *P*, with the following properties:

(0) A player wins by consistently moving to positions of *G*-value 0.

(1) $G(P) = \text{mex}\ \{ G(Q), G(R), \cdots \}$, taken over all positions Q, R, $\cdots$ obtained from *P* by a single move, where ‘‘mex’’ (or minimal excluded value) means ‘‘the smallest number (from 0,1,2,3,...) not among’’.

(2) The *G*-value of a general position $P_a + P_b + \cdots$ is given by

$$G(P_a + P_b + ...) = G(P_a) \oplus G(P_b) \oplus \cdots ,$$

where $\oplus$ is nim-addition. (The nim-sum of numbers i, j, k, $\cdots$ is obtained by writing them in binary and adding without carries, or in other words by forming the exclusive-or of their binary representations [2, p. 51]. See Table II below.)

The *G*-values of the atomic positions in Grundy’s game are given by the following table ($G(n)$ is the *G*-value of a single heap of size *n*).

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$G(n)$	0	0	1	0	2	1	0	2	1	0	2	1	3	2	1	$\cdots$

The reader will easily verify for example that a single heap of size 4, or two heaps of size 3 and 6, are winning positions.(1)

(2.3) The winning code.

Alternatively, the general position $\sum_{i=0} n_i \, P_i$ in such a game may be represented by the integral vector

$$(\cdots \; n_3 \; n_2 \; n_1 \;) \; ,$$

(or by the vector

$$(\cdots \; n_3 \; n_2 \; n_1 \; n_0 \;) \; ,$$

if the zero heaps play a significant role). However, since $x \oplus x = 0$ for all x, the outcome of such a position depends only on the parities of the n_i. The winning strategy is therefore encapsulated in a certain binary code, consisting of all vectors

$$(\cdots \; \zeta_3 \; \zeta_2 \; \zeta_1 \;), \quad \text{where} \quad \zeta_i = 0 \text{ or } 1,$$

for which the nim-sum

$$\sum \zeta_i \, G(P_i) = 0 \; . \qquad (3)$$

We call this the *winning code* for the game.

For example, in Grundy's game the first few codewords and the corresponding winning positions are shown in Table I. A vector $\cdots \; \zeta_3 \; \zeta_2 \; \zeta_1$, where $\zeta_i = 0$ or 1, is in the code if and only if

$$\zeta_1 G(1) \oplus \zeta_2 G(2) \oplus \zeta_3 G(3) \oplus \cdots = 0,$$

(1) The footnotes are on page 38.

i.e.

$$\zeta_3 \oplus 2\zeta_5 \oplus \zeta_6 \oplus 2\zeta_8 \oplus \cdots = 0 \ .$$

Since the code is defined by the linear condition (3), we deduce the following surprising result.

Theorem 1.

The winning code for a heap game is a linear code over $GF(2)$.

The codewords as just defined have infinitely many coordinates. However, for any *n*, we may obtain a code of length *n* by restricting attention to words that vanish outside the last *n* coordinates.

(2.4) Generalization to base B; lexicodes.

We now define analogs of these games (and codes) in which the number 2 is replaced by a general base *B*. Theorem 1 generalizes satisfactorily if *B* is a power of 2, but the codes seem to have little structure for other values of *B*.

In view of Eq. (3), we can regard the heap game described in Section (2.2) as played with binary numbers $N = \sum \zeta_i 2^i$, where $\zeta_i = 0$ or 1 (or with the corresponding binary vectors $(\cdots \zeta_3 \ \zeta_2 \ \zeta_1)$), and the legal move is to replace N by $N' = \sum \zeta'_i 2^i$ provided

(i) $N' < N$ (this is the *lexicographic condition*) and

(ii) the collection of i such that $\zeta'_i \neq \zeta_i$ is a turning set.

More generally, we may consider a game defined by giving a base B and a family of finite turning sets of the form

$$\{h, i, j, \cdots\} \ , \ h > i > j > \cdots \ .$$

A position is described by a number

$$N = \sum \zeta_i B^i \ , \ \zeta_i = 0, 1, \ldots, B-1,$$

written in the base B, or equivalently by a vector

$$N = (\cdots \zeta_3 \ \zeta_2 \ \zeta_1), \ \text{where} \ \ \zeta_i = 0, 1, \ldots, B-1 \ .$$

Again the legal move is to replace N by $N' = \sum \zeta'_i B^i$ provided conditions (i) and (ii) are satisfied. Thus the turning sets only specify *where* two successive positions must differ, not by how much. The Sprague-Grundy theory also applies to these games, and we may define the corresponding winning code as in Section (2.3).

For each family of turning sets and each base B we may also define another code called an (*unrestricted*) *lexicographic code*, or *lexicode*. This code is defined by the following greedy algorithm. The possible words $(\cdots \zeta_3 \ \zeta_2 \ \zeta_1)$, $0 \le \zeta_i < B$, are considered in the lexicographic order determined by the corresponding number

$$N = \sum \zeta_i B^i \ .$$

A word is rejected if there is some earlier word $N' = (\cdots \zeta'_3 \ \zeta'_2 \ \zeta'_1)$ for which the set of i with $\zeta'_i \ne \zeta_i$ is a turning set, and is otherwise accepted, i.e. placed in the code. The set of coordinates i defined by (4) will be denoted by $\Delta(N, N')$.

It turns out that this code is the same as the winning code.

Theorem 2.

For any turning set and any base, the winning moves in the game are to move to positions corresponding to the codewords in the lexicode.

Proof. The proof is by induction on N (the position). There are two things to be checked. If N is not in the lexicode, this must be because there is a smaller number N' in the lexicode for which $\Delta(N,N')$ is a turning set. Therefore, by the induction hypothesis, the move from N to N' is a winning move, and N is not a winning position. On the other hand, if N is in the lexicode, and N to N' is any legal move, then $N' < N$ and $\Delta(N,N')$ is a turning set. Since we accept N we must have rejected each such N', and so the move from N to N' cannot be a winning move. Therefore N is a winning position. This completes the proof.

(2.5) Example.

We take $B = 8$ and let the turning sets be all sets of size 1 or 2. Thus distinct codewords must differ in at least 3 places. Applying the greedy algorithm, we find that the lexicode contains the words

0000
0111
0222
. . .
0555
. . .
0777
1012
1103
. . .

Theorem 4 below shows that this code is closed under componentwise nim-addition of vectors. E.g. $0555 \oplus 1103 = 1456$ will again be in the code. (Table II below contains a nim-addition table.)

(2.6) Example.

More generally, for any base B, if the turning sets consist of all sets of cardinality $1, 2, 3, \ldots, d-1$, the corresponding lexicode is that with minimal Hamming distance d.

(2.7) Example.

For $B = d = 4$, the lexicode begins

000000
001111
002222
003333
010123
011032
012301
. . .

As in Example (2.5), this code is closed under nim-addition. But now Theorem 5 below shows that it is also closed under *nim-multiplication* by 0, 1, 2, 3, nim-multiplication being defined by

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Thus $3 \otimes (010123) = (030312)$ will also be in the code. (Nim-multiplication of numbers greater than 3 is more subtle and is described in Section (2.9).)

In fact if we stop at length 6 this code is the *hexacode*, the [6,3,4] extended ‘‘Golay’’ code over $GF(4) = \{0, 1, \omega, \bar{\omega} = \omega^2 = \omega + 1\}$, where we identify ω with 2 and $\bar{\omega}$ with 3 ([4, Eq. (7)], [7]).

(2.8) The additive theorem.

By combining Theorems 1 and 2 we immediately obtain the following result.

Theorem 3.

If $B = 2$ *the lexicode defined by any family of turning sets is a binary linear code.*

This may be generalized.

Theorem 4. **The additive theorem**.

If B is a power of 2 *the lexicode defined by any family of turning sets is closed under componentwise nim-addition.*

Proof. It will suffice to consider the case $B = 8$, the general case being exactly similar. We convert octal vectors into binary vectors by replacing each octal digit ζ_i by three binary digits $\delta_{3i+2}, \delta_{3i+1}, \delta_{3i}$ in the usual way:

ζ_i	δ_{3i+2}	δ_{3i+1}	δ_{3i}
0	0	0	0
1	0	0	1
2	0	1	0
		. . .	
7	1	1	1

In this way the original octal game becomes a binary game in which T is a turning set just if

$$\left\{ \left[\frac{i}{3} \right] : i \in T \right\}$$

was a turning set in the octal game (where $[x]$ denotes the integer part of x). The desired result now follows by applying Theorem 3 to the new binary game.

Conversely, if B is not a power of 2 then in general the lexicode is not closed under any reasonable definition of addition. For example, if $B = 3$ and the turning sets are all the sets of cardinality 1 (i.e. the code has minimal distance 2) then the lexicode begins

0000
0011
0022
0101
0110
0202
$\cdots$.

But the sum of the third and fourth words is not in the code.

(2.9) Nim-multiplication.

In any additive group the rule for addition must have the property that if

$$a \neq a' \quad \text{and} \quad b \neq b'$$

then

$$a+b \neq a'+b \quad \text{or} \quad a+b' \ .$$

Nim-addition can be defined by setting the sum of a and b equal to the lexicographically earliest value permitted by this property. More precisely, the nim-sum $a \oplus b$ (defined in Section (2.2)) can also be defined recursively by

$$a \oplus b = \operatorname*{mex}_{a' < a \;,\; b' < b} \{ \, a' \oplus b \;\; , \;\; a \oplus b' \, \} \; . \tag{5}$$

There is an operation $\otimes$ called *nim-multiplication* which together with $\oplus$ converts the integers into a field [2, Chap. 6]. In any field if $a \neq a' \;\; , \;\; b \neq b'$ then

$$(a - a') \; (b - b') \neq 0$$

and so

$$ab \neq a'b \, + \, ab' \, - \, a'b' \; ,$$

or in a field of characteristic 2

$$ab \neq a'b \, + \, ab' \, + \, a'b' \; .$$

The nim-product of a and b is the lexicographically earliest value permitted by this property. More precisely, $a \otimes b$ is defined recursively by

$$a \otimes b = \operatorname*{mex}_{a' < a,\; b' < b} \{ \, a' \otimes b \oplus a \otimes b' \oplus a' \otimes b' \, \} \tag{6}$$

(where nim-multiplication takes precedence over nim-addition). It is a remarkable fact that $\oplus$ and $\otimes$ as defined by the greedy algorithms (5) and (6) convert the numbers $0,1,2,3$,... into a field [2, p. 55]. The characteristic of this field is 2. Also, for all a, the numbers less than 2^{2^a} form a subfield isomorphic to the Galois field $GF(2^{2^a})$ [2, Theorem 49]. We have already seen an illustration of this in the case $B = 4 = 2^{2^1}$ in Example (2.7).

The nim-addition and nim-multiplication tables for numbers less than $16 = 2^{2^2}$ are given in Tables II and III [2, pp. 51,52]. In view of the previous remark, these numbers form the field $GF(16)$.

Nim-sums and products can be easily computed using the field laws and the facts that:

for N of the form 2^a we have

$$N \oplus n = N + n \quad \text{for} \quad n < N \ , \tag{7}$$

$$N \oplus N = 0 \ ; \tag{8}$$

for N of the form 2^{2^a} we have

$$N \otimes n = Nn \quad \text{for} \quad n < N \ , \tag{9}$$

$$N \otimes N = \frac{3}{2} N \ . \tag{10}$$

The standard reference for nim-multiplication is Chapter 6 of [2]. See also [1, Chap. 14], [14] and [15].

(2.10) The multiplicative theorem.

Theorem 5. **The multiplicative theorem**

If B is of the form 2^{2^a} *then the lexicode defined by any family of turning sets is closed under componentwise nim-multiplication by numbers* α *in the range* $0 \le \alpha < B$. *In other words the lexicode is a linear code over the field* $GF(2^{2^a})$.

Before giving the proof, let us define $f(\zeta, P)$ to be the G-value of the position with a single ζ $(0 \le \zeta \le B - 1)$ in coordinate P:

$$f(\zeta,P) \;=\; G(\;\cdots\; 0,0,\zeta,0\;,\ldots,\;0)\;, \tag{11}$$

and let $f(P) \;=\; f(1,P)$.

Proof. By Theorem 2 the lexicode consists of the positions with G-value zero. Therefore by the additive theorem (Theorem 4), the desired conclusion will follow if we show that

$$f(\zeta,P) \;=\; \zeta \otimes f(P) \tag{12}$$

for all ζ,P. We show this by a double induction on α and P. From Rule (1) of Section (2.2),

$$f(\zeta,P) \;=\; \underset{(13)}{\mathrm{mex}}\; \{f(\zeta\,',P) \;\oplus\; \sum\; f(\eta_i,Q_i)\}$$

where the mex is taken over these values:

$$\begin{array}{l} 0 \le \zeta\,' < \zeta, \\ \{\,P,\;Q_1,\;Q_2\;,\ldots\,\}\ \text{is a turning set}, \\ 0 < \eta_i < B\ \text{for all}\ i\;. \end{array} \tag{13}$$

(Every coordinate of the turning set must be changed.) By the induction hypothesis,

$$f(\zeta,P) \;=\; \mathrm{mex}\;\{\;\zeta\,' \otimes f(P) \;\oplus\; \sum\; \eta_i \otimes f(Q_i)\;\}\;. \tag{14}$$

On the other hand, from (6),

$$\zeta \otimes f(P) \;=\; \mathrm{mex}\;\{\;\zeta\,' \otimes f(P) \;\oplus\; (\zeta \oplus \zeta\,') \otimes \lambda\;\} \tag{15}$$

where $\zeta\,' < \zeta$ and $\lambda < f(P)$. Now

$$f(P) \;=\; \underset{(13)}{\mathrm{mex}}\;\{\;\sum\;\eta_i \otimes f(Q_i)\;\}\;,$$

so all $\lambda < f(P)$ can be written in the form $\lambda = \sum\,\eta_i \otimes f(Q_i)$. Therefore (15) becomes

$$\zeta \otimes f(P) = \operatorname*{mex}_{(13)} \{ \zeta' \otimes f(P)$$

$$\oplus \sum (\zeta \oplus \zeta') \otimes \eta_i \otimes f(Q_i) \} . \qquad (16)$$

The numbers less than B form a field, $GF(B)$, and therefore (since $\alpha \oplus \alpha'$ is a nonzero constant) the sum in (16) is equal to $\sum \eta_i \otimes f(Q_i)$. Equations (14) and (16) now agree, which establishes the desired result.

Conversely, if B is not of the form 2^{2^a}, then in general the lexicode is not closed under any reasonable definition of multiplication. This may be seen for example in the case $B = 8$ and $d = 3$; we omit the details.

III. Lexicodes

(3.1) Introduction.

In this section we discuss some particular families of lexicodes in more detail. We specify the base B, the desired minimal Hamming distance d, and take the turning sets to consist of all sets of cardinality $1, 2, \ldots, d-1$. Then the lexicode is formed by starting with the zero word, and repeatedly adjoining the lexicographically earliest word that is at Hamming distance at least d from all previous words.

As we have seen, if $B = 2^a$ the lexicode is closed under addition (Theorem 4), and if $B = 2^{2^a}$ it is also closed under multiplication by scalars, i.e. is a linear code over $GF(B)$ (Theorem 5).

A code of length n is obtained by accepting only those codewords that vanish outside the last n coordinates.

The parameters of the lexicodes are summarized in Tables IV-VII. Tables IV, V and VI give the number of codewords in the lexicodes with $d = 3,4$ and 6 respectively, for various bases and lengths. Table VII gives the dimension k of the binary ($B = 2$) lexicodes for $n \le 44$ and $d \le 10$. (In view of Example (3.2b) below, it is enough to consider even values of d.)

Table VIII shows the number of codewords in extended and/or shortened Hamming codes for the range of lengths and bases covered by Tables IV and V. Comparison of these tables shows that lexicodes are as good as Hamming codes for $B = 2^{2^a}$ (as we shall see in Theorem 6, lexicodes actually *are* Hamming codes in this case); they are usually slightly inferior to Hamming codes when $B = 2^a$ (they are *sometimes* better, for example when $B = 8$, $n = 11$, $d = 4$); and they are worse for other values of B.

If we just consider binary lexicodes, as in Table VII, comparison with the tables in [16, Appendix A] shows that the lexicodes are very good. In the range of Table VII they have dimensions within 1 or 2 of the best codes known, and often have the same dimension (see the next section).

We now discuss some of these codes in more detail.

(3.2) Some well-known codes.

We first mention that some well-known codes are lexicodes. The proofs of the following assertions will either be given later, can be found in [1], or are straightforward verifications.

(a) Zero-sum codes

For $d = 2$ and any B, the lexicode of length n is the *zero-sum* code, consisting of all vectors

$$(\zeta_{n-1} \; \zeta_{n-2} \; \cdots \; \zeta_2 \; \zeta_1)$$

for which the nim-sum $\sum \zeta_i = 0$. For example, this is the even-weight code in the binary case. We omit the easy proof by induction.

(b) Hamming codes

When $B = 2$ and $d = 3$, the turning sets have size 1 and 2, and the game is nim$^{(2)}$ itself, the oldest and best known heap game [1, p. 430]. The corresponding lexicodes of length $n = 2^m - 1$ coincide with binary Hamming codes (see Theorem 6), and those of other lengths are shortened Hamming codes. Similarly when $B = 2$, $d = 4$ and $n = 2^m$ we obtain extended Hamming codes (see (c) below). The heap game for $d = 4$ is called Mock Turtles [1, p. 431].

(c) Extended binary codes

When $B = 2$ the lexicodes with d even are obtained from the lexicodes with d odd by adding an overall parity check. This is equivalent to the ‘‘Mock Turtle Theorem’’ [1, p. 432]. So for $B = 2$ it is only necessary to consider even values of d. (This property does not hold for $B > 2$.)

(d) The extended quadratic residue code of length 18

The lexicode with $B = 2$, $d = 6$, and $n = 18$ is the [18,9,6] binary extended quadratic residue code [16, p. 483]. The corresponding game is called Moebius [1, p.

434].

(e) The extended Golay code

The lexicode with $B = 2$, $d = 8$ and $n = 24$ is the [24,12,8] binary Golay code. The corresponding game is called Mogul [1, p. 435].

(f) Binary codes with distance 10

If $B = 2$ and $d = 10$, when $n = 27$ or 31 the lexicodes have parameters [27,9,10] and [31,12,10] respectively. Codes with the same parameters were constructed by Hashim and Constantinides [12] and Piret [17]. The corresponding game is Moidores.

(g) The tetracode

Taking $B = d = 3$, $n = 4$ we obtain the [4,2,3] code over $GF(3)$ sometimes called the tetracode ([4, p. 321], [7]). The nine codewords are

0000	1012	2021
0111	1120	2102
0222	1201	2210

This code is ‘‘accidentally’’ linear over $GF(3)$. (See Table XI for the continuation.)

(h) The hexacode

As already mentioned in Section (2.7), when $B = d = 4$ and $n = 6$ we obtain the [6,3,4] hexacode over $GF(4)$.

(3.3) The case $B = 2^a$

When $B = 2^a$ the lexicode may be efficiently specified by giving the values of the function $f(\zeta, i)$ (the G-value of a position in which there is a single nonzero digit ζ, $0 \leq \zeta \leq B-1$, in coordinate i - see Eq. (11)). It is convenient to write $f(\zeta, i)$ in the base B.

For example when $B = 8$ and $d = 3$ the values of $f(\zeta, i)$ are shown in Table IX, written in octal.

To illustrate how this table was obtained, we derive the entry $f(2,3) = 023$. From the position

$$\begin{array}{cccccc} & {\scriptstyle 4} & {\scriptstyle 3} & {\scriptstyle 2} & {\scriptstyle 1} & {\scriptstyle 0} \\ \left[\cdots \right. & 0 & 2 & 0 & 0 & \left. 0 \right] \end{array}$$

we can move to any of

$$\begin{array}{l} (\ldots\ 0\ x\ 0\ 0\ y) \\ (\ldots\ 0\ x\ 0\ y\ 0) \\ (\ldots\ 0\ x\ y\ 0\ 0) \end{array}$$

where $x = 0,1$, $y = 0,1, \ldots, 7$ (since the turning sets are of size 1 and 2). So $f(2,3)$ is the mex of

$$\begin{cases} f(0,3) \oplus abc = 000 \oplus abc \\ f(1,3) \oplus abc = 012 \oplus abc \end{cases} \tag{17}$$

where $abc = f(y,0)$, $f(y,1)$ or $f(y,2)$ is any entry from the first three rows of Table IX. It is easily checked that the first octal number not of the form (17) is 023.

The additive property (Theorem 4) implies that the columns for $\zeta = 1,2$ and 4 determine the others. The typical entry in the $\zeta = 6$ column for example is the nim-sum of the entries in columns 2 and 4.

By Theorem 2, the codewords are the positions of G-value zero. We illustrate how the codewords are found from the $f(\zeta, i)$ table by an example. For what values of x and y is

$$\ldots 0 \ldots 020xy$$

a codeword? Since

$$f(2,3) = 023,\ f(x,1) = 0x0,\ f(y,0) = 00y$$

(from Table IX), the answer is $x = 2,\ y = 3$, i.e.

$$\ldots 0 \ldots 02023\ .$$

In this way, if d is small, it is easy to obtain the number of codewords and a basis directly from the table. The codes in the $B = 8$ column of Table IV and V were found in this way.

These codes are comparable in efficiency with Reed-Solomon codes, and of course exist for all lengths (whereas Reed-Solomon codes only exist for lengths up to $B+1$ or $B+2$ [16, p. 317]). For example, when $d = 3,\ B = 8$, if the lexicode contains 2^{k_l} codewords and the Reed-Solomon code contains 2^{k_R} codewords, we have

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k_l	3	5	8	11	14	17	20	23	25	28	31	34	37	40
k_R	3	6	9	12	15	18	21							

(This is a continuation of the $B = 8$ column in Table IV.)

(3.4) The case $B = 2^{2^a}$

The multiplicative property of Theorem 5 makes it even easier to construct the lexicode in the case when B is of the form 2^{2^a}, since Eq. (12) holds. This property was used in calculating the extensive table of G-values for the case $B = 2$ given on p. 433 of [1]. Table VII above was then derived from that table.

One can also use (12) to establish the following result.

Theorem 6

In the case $B = 2^{2^a}$, $d = 3$, *lexicodes of length*

$$n = 1 + B + B^2 + ... + B^{m-1} = \frac{B^m - 1}{B - 1}$$

are Hamming codes, and those of other lengths are shortened Hamming codes.

We omit the proof.

As mentioned in Example (3.2c), the lexicode with $B = 2$ and d even is obtained by adding an overall parity check to the lexicode with $B = 2$ and distance $d - 1$. So as far as the earliest families of lexicodes are concerned, we have a complete theory in the cases B arbitrary, $d = 2$ (zero-sum codes, (3.2a)), $B = 2$, $d = 3$ (binary Hamming codes, (3.2b)), $B = 2$, $d = 4$ (extended binary Hamming codes, (3.2b)), and $B = 4$, $d = 3$ (Hamming codes over $GF(4)$, (Theorem 6)).

The structure of the next family of lexicodes, for $B = d = 4$, has been determined by R. A. Wilson [22]. Let us define a *Wilson number* to be one whose base-4 expansion is either 1 or 10, or else has the form $\zeta_m \ \zeta_{m-1} \ \cdots \ \zeta_2 \ \zeta_1 \ \zeta_0$ (for $m \geq 2$) where

$$
\begin{aligned}
\zeta_m &= 1 \, , \\
\zeta_i &= 0 \text{ or } 1 \quad \text{for } m > i \geq 2, \\
\zeta_1 &= 0,\ 1,\ 2 \text{ or } 3, \\
\zeta_0 &= 1 + \zeta_1^2 + \zeta_2^2 + \cdots + \zeta_m^2 \, ,
\end{aligned}
\tag{18}
$$

where the addition and multiplication in (18) are in the nim sense. The first few Wilson numbers (written in base 4) are

$$
\begin{aligned}
&1,\ 10,\ 100,\ 111,\ 123,\ 132,\ 1000,\ 1011,\ 1023, \\
&1032,\ 1101,\ 1110,\ 1122,\ 1133,\ 10000, \ldots
\end{aligned}
$$

Theorem 7 *(R. A. Wilson* [22]*)*

The G-value ($f(1,i)$) *of the position* $\cdots\ 0,1,0, \ldots, 0$ *(with a single* 1 *in the* i^{th} *coordinate) is the i-th Wilson number.*

Thus $G(\cdots 0001) = 1$, $G(\cdots 0010) = 10$, $G(\cdots 0100) = 100$, $G(\cdots 1000) = 111$, etc. (in base 4).

For completeness we include a proof in our terminology.

Important Note. With the single exception that 4^i means the usual *i*-th power of 4, all additions and multiplications in the proof are in the nim sense.

Proof. The proof is by induction. Suppose we have checked that the first *k* *G*-values are the first *k* Wilson numbers $W_0, \ldots, W_{k-1}$. We must show that the next number

$$
n = \sum_{i=0}^{m} 4^i \ \delta_i \tag{19}
$$

that is not a linear combination of two of $W_0, \ldots, W_{k-1}$ is the next Wilson number W_k.

(i) If some δ_i $(i \geq 2)$ in (19) is 2 or 3 then *n is* a linear combination of two of $W_0, \ldots, W_{k-1}$. For we may obtain *n* as

$$N = 2p + 3q \tag{20}$$

where

$$p = \sum_{i=2}^{m} 4^i \alpha_i + 4\alpha + (\alpha^2 + \theta_1) ,$$

$$q = \sum_{i=2}^{m} 4^i \beta_i + 4\beta + (\beta^2 + \theta_2) ,$$

$$\theta_1 = \sum_{i=2}^{m} \alpha_i^2 + 1 , \quad \theta_2 = \sum_{i=2}^{m} \beta_i^2 + 1 ,$$

and where we choose α_i and β_i according to

d_i	0	1	2	3
α_i	0	1	1	0
β_i	0	1	0	1

for $m \geq i \geq 2$. Then α and β are uniquely determined by

$$2\alpha + 3\beta = \delta_1 , \tag{21}$$

$$2\alpha^2 + 3\beta^2 = \delta_0 + 2\theta_1 + 3\theta_2 . \tag{22}$$

Since we are working in the field $GF(4)$, (21) and (22) can be solved for α and β. It is easy to check that with these values of *p* and *q*, *n* is given by Eq. (20). *p* and *q* are Wilson numbers, and, since some $\delta_i (i \geq 2)$ is 2 or 3, $p \neq q$.

(ii) We next check that no Wilson number is a linear combination of two earlier Wilson numbers. Suppose on the contrary that $n = ap + bq$, where *n* is given by (19) and

$$p = \sum_{i=0}^{m} 4^i \alpha_i \quad , \quad q = \sum_{i=0}^{m} 4^i \beta_i \ .$$

There are two cases. (a) If $\alpha_m = \beta_m = 1$, we must have $\{a,b\} = \{2,3\}$, say $a = 2$, $b = 3$. Since $\delta_{m-1}, \ldots, \delta_2$ are 0 or 1, we must have $\alpha_{m-1} = \beta_{m-1}, \ldots, \alpha_2 = \beta_2$. Then

$$\begin{aligned}\delta_0 &= \sum_{i=1}^{m-1} \delta_i^2 = \sum_{i=1}^{m-1} (2\alpha_i + 3\beta_i)^2 \\ &= 3 \sum_{i=1}^{m-1} \alpha_i^2 + 2 \sum_{i=1}^{m-1} \beta_i^2 \\ &= 3\,\alpha_0 + 2\,\beta_0 \ .\end{aligned}$$

But also $\delta_0 = 2\,\alpha_0 + 3\,\beta_0$, implying $\delta_0 = \alpha_0 = \beta_0$. Therefore $\alpha_1 = \beta_1$, hence $p = q$, so $n = p = q$, contradicting $n > p$. (b) If $\alpha_m = 1$, $\beta_m = 0$, we must have $a = 1$, $b = 0$, and then

$$\begin{aligned}\delta_0 &= \alpha_m^2 + \cdots + (\alpha_1 + \beta_1)^2 \\ &= (\alpha_m^2 + \cdots + \alpha_1^2) + (1^2 + \cdots + \beta_1^2) \\ &= (\alpha_0 + 1) + \beta_0 \ ,\end{aligned}$$

which contradicts $\delta_0 = \alpha_0 + \beta_0$.

(iii) If all δ_i $(i \geq 2)$ in (19) are 0 or 1, n has the form

$$n = \sum_{i=2}^{m} 4^i \delta_i + 4\,\zeta + \xi \quad , \quad (\delta_i = 0 \text{ or } 1) \ . \tag{23}$$

We must show that the next numbers of this form that are not linear combinations of two earlier Wilson numbers are Wilson numbers. In other words, we must show that if the number of 1's in $\{\delta_m, \delta_{m-1}, \ldots, \delta_2\}$ is odd (resp. even) then (ζ,ξ) runs through

$$\begin{matrix} 0,0 \\ 1,1 \\ 2,3 \\ 3,2 \end{matrix} \qquad \left[\text{resp. } \begin{matrix} 0,1 \\ 1,0 \\ 2,2 \\ 3,3 \end{matrix} \right] .$$

Let

$$n' = \sum_{i=2}^{m} 4^i \delta_i \ . \tag{24}$$

If the number of 1's in n' is odd, then the earliest numbers of the form (23) that are accepted are

$$p = n' + 4 \otimes 0 + 0$$

(this is a Wilson number, and by (ii) it is accepted), and

$$q = n' + 4 \otimes 1 + 1$$

(this is the smallest number that differs from p in two coordinates). Then

$$n' + 4 \otimes 2 + 2 = 3p + 2q$$

is excluded, but

$$r = n' + 4 \otimes 2 + 3 \ ,$$

$$s = n' + 4 \otimes 3 + 2$$

are accepted. On the other hand, suppose the number of 1's in n' is even. We can write

n
matrix {
lcol {4 ^ citimes ^ 0 ~+~ 0 above 4 ^ citimes ^ 1 ~+~ 1 above 4 ^ citime
}

$n' = n$ where the numbers of ones in n are odd. Then are earlier Wilson numbers. Adding, we see that

$$n' + \begin{cases} 4 \otimes 0 + 0 \\ 4 \otimes 1 + 1 \\ 4 \otimes 2 + 3 \\ 4 \otimes 3 + 2 \end{cases}$$

are excluded, and so we must go to at least

$$p = n' + 4 \otimes 0 + 1 \ ,$$

$$q = n' + 4 \otimes 1 + 0 \ ,$$

$$r = n' + 4 \otimes 2 + 2 \ ,$$

$$s = n' + 4 \otimes 3 + 3 \ .$$

Since these are Wilson numbers, by part (ii) they are accepted. This completes the proof.

Corollary 8

For $B = d = 4$*, the lexicode of length* $n = 2^m - 2$ *contains* 4^k *codewords, where* $k = 2^m - m - 2$.

The case $m = 3$ is described in Example (3.2h).

Wilson's theorem does not hold for $B = 2^{2^a} > 4$ and $d = 4$. The first few G-values $f(1, i)$ are shown in Table X, and the last entry in the table does not have the form of a Wilson number.

(3.5) Other values of B

Lexicodes in general appear to have little or no structure. This can already be seen in the case $B = d = 3$. The numbers of codewords in the first few codes are given in Table IV, and the complete code of length 8 is shown in Table XI. We have been unable to discover any structure to this code (or the solution of the corresponding game).

IV. Constant weight lexicographic codes

(4.1) Introduction

A *constant weight lexicode* is defined similarly: we consider all words of the specified weight in lexicographic order, and accept a word if it is at Hamming distance at least d from all previously accepted words. Only binary codes will be considered here. The Hamming distance d is necessarily even. To distinguish these codes from the lexicodes of Section III we refer to the latter as *unrestricted* lexicodes.

The game corresponding to a constant weight lexicode of weight w and minimal distance $d = 2t \geq 4$ is the following. The typical position is a set $\{ a_1 , a_2 , \ldots , a_w \}$ of distinct nonnegative integers, and the legal move is to decrease $1, 2, \ldots,$ or $t - 1$ of these integers while preserving their distinctness. As always, the first player who is unable to move loses. (These games are no longer well described by turning sets.) Again the Sprague-Grundy theory applies, and we may define the corresponding winning code as in Section (2.3).

Theorem 9

For any $d = 2t \geq 4$ and any w, the winning code for this game is the constant weight lexicode with the same parameters.

The proof is analogous to that of Theorem 2 and is omitted.

(4.2) The case $d = 2$.

The condition $d = 2$ is automatically satisfied, and the corresponding lexicode consists of all codewords of weight w.

(4.3) The case $d = 4$.

The constant weight lexicode for $d = 4$ and any w is the winning code for *Welter's game* [1, pp. 472-481], [2, Chap. 13], [20], [21]. This is the only other case (besides $d = 2$) where there is a complete theory.

Welter's game is the case $t = 2$ of the game described in Section (4.1). A typical position is a set $\{ a_1 , a_2 , \ldots , a_w \}$ of distinct nonnegative integers, and the legal move is to decrease one of these integers while preserving their distinctness. The complete solution [1, pp. 472-481], [2, Chap. 13] uses Welter's remarkable function $W(a_1, a_2, \ldots, a_w)$, which can be defined recursively by

$$W(a_1) = a_1 , \tag{25a}$$

$$W(a_1, a_2) = (a_1 \oplus a_2) - 1 \tag{25b}$$

and

$$\begin{aligned} & W(a_1, \ldots, a_{k+1}) \\ & = W(a_2, \ldots, a_k) \oplus \left[(W(a_1, \ldots, a_k) \oplus W(a_2, \ldots, a_{k+1})) - 1 \right] . \end{aligned} \tag{25c}$$

The -1 in (25) is ordinary subtraction, so the definition of W mixes nim-addition and ordinary subtraction.

Theorem 10

$(a_1, \ldots, a_w)$ is a winning position for Welter's game, or equivalently the vector with 1's in positions $a_1, \ldots, a_w$ is in the lexicode with constant weight w and minimal distance 4, if and only if

$$W(a_1, \ldots, a_w) = 0 .$$

As we shall see, Theorem 10 is a consequence of the following property of Welter's function.

Theorem 11. The even alteration property.

If $W(a_1, \ldots, a_w) = n$, and $n' \neq n$, there are unique nonnegative numbers $a'_1, \ldots, a'_w$ such that $a_1, \ldots, a_w, a'_1, \ldots, a'_w$ are distinct and satisfy

$$W(a'_1 \ , a_2 \ , \ldots , \ a_w) \ = \ n' \ ,$$

$$W(a_1 , \ a'_2 \ , \ldots , \ a_w) \ = \ n' \ ,$$

...

$$W(a_1 , \ a_2 \ , \ldots , \ a'_w) \ = \ n' \ .$$

More generally

$$W(a_1 , \ a_2 \ , \ldots , \ a_w) \ = \ n$$

remains true if any even number of the letters $a_1 , \ldots , a_w$, n *are replaced by the corresponding sup primed letters. Furthermore an even number of the inequalities*

$$a'_1 \ < \ a_1 \ ,$$

$$a'_2 \ < \ a_2 \ ,$$

$$\ldots$$

$$a'_w \ < \ a_w \ ,$$

$$n' \ < \ n$$

are true.

For the proof see [2, Chap. 13]. When $n \neq 0$, if we take $n' = 0$ we see that there is always at least one $a'_i < a_i$, and so it is always possible to move from a position in which $W(a_1 , \ldots , a_w) \neq 0$ to a position in which $W(a_1 , \ldots , a_w) = 0$. Theorem 10 follows.

The calculation of Welter's function from (25) is best carried out using the tableau shown in Fig. 1 (cf. [1, p. 476]). Notice that once the first two rows are filled in (using (25a)), the tableau may be completed by the rule that any four entries arranged in a diamond

$$\begin{array}{ccc} & A & \\ B & & C \\ & D & \end{array} \tag{26a}$$

must satisfy

$$A \oplus D = (B \oplus C) - 1 . \tag{26b}$$

Remarks (i) A tableau satisfying such a rule is called a *frieze pattern*. They have interesting properties in the cases $f(x,y) = xy,\ x + y,\ x \oplus y$; see [1, p. 475],[3].

(ii) Although it is not apparent from (25), Welter's function is a symmetric function of its arguments. For this and other combinatorial properties see [2, Chap. 13].

Theorem 9 guarantees that if a vector ζ is not in the code, there is a codeword within Hamming distance 3 that is earlier than ζ in the lexicographic order. To find a winning move $a_i \to a'_i$, and hence to *decode* ζ, it is again convenient to use a frieze pattern (cf. [1, p. 477]).

We illustrate the decoding (or winning) strategy with an example. Suppose $w = 5$, we are given a,b,c,d,e and n,n', and wish to find a', b', c', d', e' as in Theorem 11. That theorem implies that if we place the numbers $a,b\ , \ldots ,\ d',e'$ in the first row of the tableau, and the numbers $n,\ n'$, $n,\ n'$,... in the fifth row, as in Figure 2, the frieze rule (26) will still hold. So we may compute a', b', c', d', e' by working downwards in the left half of the tableau and upwards in the right half, as illustrated by the numerical example in Fig. 3. Here $a = 2$, $b = 3$, $c = 5$, $d = 7$, $e = 11$, $n = 4$ and $n' = 0$. Figure 3 shows that the winning move is from $\{2,3,5,7,11\}$ to $\{1,2,3,7,11\}$, i.e. that

$$\ldots\ 100010101100$$

should be decoded as

$$\ldots\ 100010001110\ .$$

For $d = 4$, $w = 3$ and $n = 2^m - 1$, the words in the constant weight lexicode are the vectors of weight 3 in the Hamming code of length $2^m - 1$. For $d = w = 4$ and $n = 2^m$, the lexicode consists of the weight 4 vectors in the extended Hamming code of length 2^m. These two assertions follow from the fact that Welter's game for $w = 3$ and 4 is equivalent to nim [1, p. 473].

Table XII gives the number of codewords in the first few constant weight lexicodes with $d = 4$. These values are of course lower bounds on the quantity $A(n, 4, w)$, where $A(n, d, w)$ is the size of the largest possible code of length *n*, constant weight *w*, and minimal distance *d*. However, in this case (for $d = 4$), these codes are in general inferior to codes already known (compare Table I of [8]).

(4.4) Other values of d; S(5,8,24)

In Section (4.3) we saw that Welter's game gives the structure of constant weight lexicodes with minimal distance 4. We have made extensive computations for other minimal distances, but although there are many interesting special cases, the resulting codes apparently display no general structure.

One interesting case occurs when $w = d = 8$. We recall from Example (3.2e) that the unrestricted lexicode for base $B = 2$, $d = 8$ and length 24 is the binary Golay code containing

1	word of weight	0
759	words of weight	8
2576	words of weight	12
759	words of weight	16
1	word of weight	24

Our computations show that at length 24 the constant weight lexicode with $w = d = 8$ consists precisely of the 759 weight 8 codewords in the full code.

Thus we have the following surprising fact.

Theorem 12.

The words of the constant weight lexicode with $w = d = 8$ and $n = 24$ are the blocks (or octads) of a Steiner system[(3)] $S(5,8,24)$.

However, for $w = 12$ and $d = 8$, there are only 481 codewords of length 24, instead of the 2576 in the Golay code. For $w = 16$ and $d = 8$, the constant weight lexicode does indeed contain 759 codewords. However, they are not precisely the 759 weight 16 words of the unrestricted $d = 8$ lexicode, but rather these words changed by the coordinate permutation

$$(0)(1) \ \cdots \ (19)(20 \quad 23)(21 \quad 22) \ .$$

(4.5) Constant weight lexicodes with a sum constraint; S(5,6,12).

In view of Theorem 11 it is natural to ask if there is a similar definition for Mathieu's other famous Steiner system, $S(5,6,12)$. The correct answer to this question emerged from some calculations of A. J. E. Ryba [18], which showed that this Steiner system can be obtained if a side condition is imposed on the lexicode.

A *constant weight lexicode with sum s* is a constant weight lexicode as in Section (4.1), with the additional requirement that every codeword

$$\cdots \zeta_3 \ \zeta_2 \ \zeta_1 \ \zeta_0$$

must satisfy

$$\sum_i i\zeta_i \geq s \ , \tag{27}$$

where the sum is calculated as an ordinary integer. In other words (since the ζ_i are 0 or 1), the sum of the w coordinates where the 1's are located must be at least s. Since every set of size w sums to at least $\begin{bmatrix} w \\ 2 \end{bmatrix}$, the sum constraint is vacuous if $s \leq \begin{bmatrix} w \\ 2 \end{bmatrix}$.

Then Ryba's discovery is the following.

Theorem 13. (Ryba [18].)

The words of the constant weight lexicode with $w = 6$, $d = 4$, $n = 12$ *and sum constraint* $s = 21$ *are the blocks (or hexads) of a Steiner system* $S(5,6,12)$.

This may be easily verified by computer. Furthermore the hexads are obtained with the so-called ‘‘shuffle labeling’’ described in [7, Chap. 12].

Mathematical Blackjack (or Mathieu's Vingt-et-un)

The game for which this code (i.e. the hexads of $S(5,6,12)$) gives the winning positions may be called Mathematical Blackjack, or Mathieu's Vingt-et-un. Six cards from a deck of 12 cards labeled $\{0,1,2, \ldots, 11\}$ are laid out face upwards on the table. The two players move alternately, the move being to replace one of the laid out cards with any lower one chosen from the remainder of the deck. The first player to make the sum less than 21 loses. Then Theorem 13 is equivalent to the assertion that the winning strategy is always to move to a hexad from $S(5,6,12)$.

(4.6) Further examples; new lower bounds to $A(n,10,w)$

The only example of a constant weight lexicode with a sum constraint for which we have a general theoretical result is the case $d = 4$, $s = \left\lfloor \frac{w}{2} \right\rfloor + 1$. It can be shown that the codewords in this case are the winning positions in the *misère* version of Welter's game [1, pp. 480-481]. We omit the details.

When $d = 10$, we discovered by experimenting that constant weight lexicodes with a sum constraint in many cases improved on the best previously known lower bounds for $A(n,10,w)$ as given in [8, Table IV]. The results are shown in Table XIII. We also take the opportunity to correct an error in Table IV of [8]: the value of $A(16,10,7)$ should be 4 (not 3).

Finally, we also experimented with applying a sum constraint to unrestricted lexicodes, but only found one code worth mentioning. When $B = 2$, $d = 3$, $n = 8$ and $s = 21$, the corresponding lexicode contains 18 codewords. This is better than any linear code, although not as good as Julin's optimal code [13] with 20 words.

Acknowledgements

We thank A. J. E. Ryba for allowing us to include his result.

List of Footnotes

(1) $G(n)$ has been calculated for $n \leq 10^7$, but it is not even known if it is eventually a periodic function of *n* [1, pp. 96, 111], [10], [11].

(2) This version of nim is also called Turning Turtles [1, p. 429].

(3) Defined on p. 59 of [16], for example.

List of Table Captions

Table I. First few codewords and corresponding winning positions in the code for Grundy's game.

Table II. Nim-addition of numbers 0 to 15.

Table III. Nim-multiplication of numbers 0 to 15.

Table IV. Number of codewords in lexicode of base *B*, length *n* and minimal distance $d = 3$. The continuation of the $B = 8$ column can be found in Section (3.3).

Table V. Number of codewords in lexicode of base *B*, length *n* and minimal distance $d = 4$.

Table VI. Number of codewords in lexicode of base *B*, length *n* and minimal distance $d = 6$.

Table VII. Binary lexicodes. The table gives the dimension k of binary $[n,k,d]$ lexicodes for $n \leq 44$ and $d \leq 10$.

Table VIII. Number of codewords in Hamming code of base *B* and length *n* (using the first column); also number of codewords in extended Hamming code of base *B* and length *m* (using the last column).

Table IX. *G*-values $f(\zeta,i)$ of coordinate positions for the case $B = 8$, $d = 3$. The *G*-values are written in octal.

Table X. *G*-values $f(1,i)$ for case $B = 2^{2^a} > 4$, $d = 4$. Here α is any digit $0,1, \ldots, B-1$, and all additions and multiplications are in the nim sense.

Table XI. The 198 words of the lexicode of length 8, distance $d = 3$ and base $B = 3$.

Table XII. Number of codewords in constant weight lexicodes with $d = 4$.

Table XIII. New lower bounds on $A(n,10,w)$ obtained from constant weight lexicodes with sum constraint s. [After this work was completed L. Hemachandra and V. K. Wei (personal communication) used the method of simulated annealing to show that $A(23,10,7) \geq 18$, $A(23,10,8) \geq 28$ and $A(24,10,8) \geq 33$.]

Table I

codeword	heap sizes
...0000000	0
...0000001	1
...0000010	2
...0000011	2,1
...0001000	4
...0001001	4,1
...0001010	4,2
...0001011	4,2,1
...0100100	6,3
...1000000	7
...	...

Table II

⊕	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Table III

⊗	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9

Table IV

$n \backslash B$	2	3	4	5	6	7	8	9	10	15	16	17
3	2	3	4	5	6	7	8	9	10	15	16	17
4	2	9	16	17	22	25	32	48	70	187	256	257
5	4	9	64	74	112	182	2^8	372	532			
6	8	24	64	265	618	1175	2^{11}					
7	16	72	2^8	1113	2994		2^{14}					
8	16	198	2^{10}				2^{17}					
9	32	519	2^{12}				2^{20}					
10	64	1390	2^{14}				2^{23}					
11	128	3650	2^{16}				2^{25}					

Table V

$n \backslash B$	2	3	4	5	6	7	8	9	10
4	2	3	4	5	6	7	8	9	10
5	2	3	16	17	18	27	32	33	46
6	4	10	64	67	88	147	2^8	314	446
7	8	24	64	165	390	766	2^{11}		
8	16	60	2^8	676			2^{14}		
9	16	136	2^{10}				2^{16}		
10	32	334	2^{12}				2^{19}		
11	64	807	2^{14}				2^{22}		

Table VI

$n \backslash B$	2	3	4	5	6	7	8
6	2	3	4	5	6	7	8
7	2	3	4	5	12	25	32
8	2	9	16	33	58	95	256
9	4	17	64	99	222		
10	4	29	256				
11	8	59					
12	16	124					
13	16	269					

Table VII

$n \backslash d$	4	6	8	10	$n \backslash d$	4	6	8	10
4	1	0	0	0	25	19	14	12	7
5	1	0	0	0	26	20	15	12	8
6	2	1	0	0	27	21	16	12	9
7	3	1	0	0	28	22	17	13	9
8	4	1	1	0	29	23	18	13	10
9	4	2	1	0	30	24	19	14	11
10	5	2	1	1	31	25	19	15	12
11	6	3	1	1	32	26	20	16	12
12	7	4	2	1	33	26	21	16	13
13	8	4	2	1	34	27	22	17	14
14	9	5	3	1	35	28	23	18	14
15	10	6	4	2	36	29	24	19	15
16	11	7	5	2	37	30	25	20	16
17	11	8	5	2	38	31	26	21	17
18	12	9	6	3	39	32	27	22	17
19	13	9	7	3	40	33	27	23	18
20	14	10	8	4	41	34	28	23	19
21	15	11	9	5	42	35	29	24	20
22	16	12	10	5	43	36	30	25	21
23	17	12	11	6	44	37	31	26	21
24	18	13	12	6					

Table VIII

$n \backslash B$	2	3	4	5	7	8	9	m
3	2	3	4	5	7	8	9	4
4	2	9	16	25	49	64	81	5
5	4	9	64	125	343	512	729	6
6	8	27	64	625	7^4	8^4	9^4	7
7	16	81	4^4	625	7^5	8^5	9^5	8
8	16	243	4^5	5^5	7^6	8^6	9^6	9
9	32	729	4^6	5^6	7^6	8^7	9^7	10
10	64	2187	4^7	5^7	7^7	8^7	9^8	11
11	128	6561	4^8	5^8	7^8	8^8	9^8	12

Table IX

$i \setminus \zeta$	0	1	2	3	4	5	6	7
0	000	001	002	003	004	005	006	007
1	000	010	020	030	040	050	060	070
2	000	011	022	033	044	055	066	077
3	000	012	023	031	100	112	123	131
4	000	013	021	032	104	117	125	136
5	000	014	042	056	101	115	143	157
6	000	015	041	054	105	110	144	151
7	000	016	045	053	107	111	142	154
8	000	017	046	051	103	114	145	152
9	000	024	043	067	102	126	141	165
10	000	025	047	062	200	225	247	262

Table X

1
B
$B^2 + \alpha B + \alpha$
$B^3 + \alpha B + \alpha^2$
$B^3 + B^2 + \alpha B + \alpha^2 + 1$
$B^4 + \alpha B + \alpha^2$
$B^4 + B^2 + \alpha B + \alpha^2 + 1$
$B^4 + B^3 + B^2 + \alpha B + \alpha^2$
$B^4 + 2B^3 + 4B^2$
...

Table XI

00000000	01100010	02201020	10221212	12121022	21020101
00000111	01100101	02202012	11000001	12122212	21021022
00000222	01101002	02202121	11000110	12201001	21022211
00001012	01101220	02210220	11001020	12201122	21100202
00001120	01102122	02211112	11001102	12202210	21102100
00001201	01102211	02212202	11001211	12210011	21120221
00002021	01120112	10010010	11002012	12212022	21122012
00002102	01121011	10010101	11002121	12220201	21200111
00002210	01121100	10011002	11002200	20010021	21200220
00110001	01122020	10011220	11110000	20010212	21210102
00110110	01122202	10012122	11110111	20011111	21212121
00111020	01200022	10012211	11110222	20012100	21221201
00111102	01201110	10020112	11111012	20020002	22000011
00111211	01202000	10020221	11111120	20020120	22001000
00112012	01211021	10021011	11111201	20021210	22001112
00112121	01211200	10021100	11112021	20101021	22001221
00112200	01221122	10022020	11112102	20102201	22002101
00120022	01222210	10022202	11112210	20110220	22011120
00210122	02012000	10100002	11200212	20120011	22012012
00220010	02012221	10100120	11220002	20121000	22020222
00220101	02020012	10100211	11220120	20121112	22022021
00221002	02021001	10101010	11221010	20122222	22022200
00221220	02021110	10101101	11222101	20200012	22100110
00222112	02022122	10101222	11222222	20200100	22102022
01010002	02100021	10102112	12000022	20201211	22110002
01010120	02100200	10120200	12010200	20202020	22110121
01010211	02101111	10122001	12011021	20211001	22111010
01011010	02110212	10200021	12011212	20211222	22112211
01011101	02120120	10201200	12012110	20212210	22121202
01011222	02121221	10210202	12102000	21000122	22220000
01012112	02122101	10211110	12102221	21012001	22220112
01020021	02200102	10212000	12120010	21012220	22221011
01020200	02200211	10221121	12120102	21020010	22222120

Table XII

$n \setminus w$	2	3	4	5	6	7	8	9
4	2	1	1					
5	2	2	1	1				
6	3	4	3	1	1			
7	3	7	7	3	1	1		
8	4	7	14	7	4	1	1	
9	4	8	14	14	8	4	1	1
10	5	10	18	22	18	10	5	1
11	5	13	26	34	34	26	13	5
12	6	17	39	54	68	54	39	17

Table XIII

$A(21,10,9) \geq 26$	(use $s = 59$)
$A(22,10,9) \geq 31$	(use $s = 70$)
$A(22,10,10) \geq 39$	(use $s = 92$)
$A(23,10,7) \geq 17$	(use $s = 58$)
$A(23,10,8) \geq 27$	(use $s = 54$)
$A(23,10,9) \geq 39$	(use $s = 74$)
$A(23,10,10) \geq 50$	(use $s = 75$)
$A(23,10,11) \geq 53$	(use $s = 80$)
$A(24,10,8) \geq 32$	(use $s = 54$)
$A(24,10,9) \geq 49$	(use $s = 65$)
$A(24,10,10) \geq 64$	(use $s = 82$)
$A(24,10,11) \geq 75$	(use $s = 79$)
$A(24,12,12) \geq 80$	(use $s = 96$)

List of Figure Captions

Figure 1. Tableau for calculation of Welter's function. The entries are calculated by $W(a_i) = a_i$ and the frieze rule (26).

Figure 2. Tableau for decoding.

Figure 3. Illustration of decoding technique in the case $w = 5$. The arrows indicate the order in which the entries are computed, using (26).

References

1. E. R. Berlekamp, J. H. Conway and R. K. Guy, *Winning Ways*, Academic Press, N.Y., 1982, 2 vols.

2. J. H. Conway, *On Numbers and Games*, Academic Press, N.Y., 1976.

3. J. H. Conway and H. S. M. Coxeter, *Triangulated polygons and frieze patterns*, Math. Gazette **57** (1973), 87-94 and 175-183.

4. J. H. Conway, V. Pless and N. J. A. Sloane, *Self-dual codes over GF(3) and GF(4) of length not exceeding 16*, IEEE Trans. Information Theory, **IT-25** (1979), 312-322.

5. J. H. Conway and N. J. A. Sloane, *Laminated lattices*, Annals of Math. (2) **116** (1982), 593-620.

6. J. H. Conway and N. J. A. Sloane, *Complex and integral laminated lattices*, Trans. Amer. Math. Soc., **280**, (1983), 463-490.

7. J. H. Conway and N. J. A. Sloane, *The Leech Lattice, Sphere Packings, and Related Topics*, Springer-Verlag, 1986, to appear.

8. R. L. Graham and N. J. A. Sloane, *Lower bounds for constant weight codes*, IEEE Trans. Information Theory, **IT-26** (1980), 37-43.

9. P. M. Grundy, *Mathematics and games*, Eureka, **2** (1939), 6-8; reprinted ibid., **27** (1964), 9-11.

10. M. J. T. Guy, unpublished.

11. R. K. Guy and C. A. B. Smith, *The G-values for various games*, Proc. Camb. Math. Soc., **52** (1956), 514-526.

12. A. A. Hashim and A. G. Constantinides, *Some new results on binary linear block codes*, Electronics Letters, **10** (1974), 31-33.

13. D. Julin, *Two improved block codes*, IEEE Trans. Information Theory, **IT-11** (1965), 459.

14. H. W. Lenstra, Jr., *On the algebraic closure of two*, Konink. Nederl. Akad. Wetensch. Proc., **A80** (1977), 389-396.

15. H. W. Lenstra, Jr., *Nim multiplication*, in *Séminaire de Théorie des Nombres* 1977-1978, Centre National de Recherche Scientifique, Talence, 1978, Exp. no. 11.

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

17. P. Piret, *Good block codes derived from cyclic codes*, Electronics Letters, **10** (1974), 391-392.

18. A. J. E. Ryba, personal communication.

19. R. P. Sprague, *Über mathematische Kampfspiele*, Tôhoku Math. J., **41** (1935-6), 438-444.

20. C. P. Welter, *The advancing operation in a special abelian group*, Koninkl. Nederl. Akad. Weten. Proc., **A55** (1952), 304-314.

21. C. P. Welter, *The theory of a class of games on a sequence of squares, in terms of the advancing operation in a special group*, Koninkl. Nederl. Akad. Weten. Proc.,

A57 (1954), 194-200.

22. R. A. Wilson, *On lexicographic codes of minimal distance 4,* Atti Sem. Mat. Fis. Univ. Modena, to appear.