Register No. 2

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

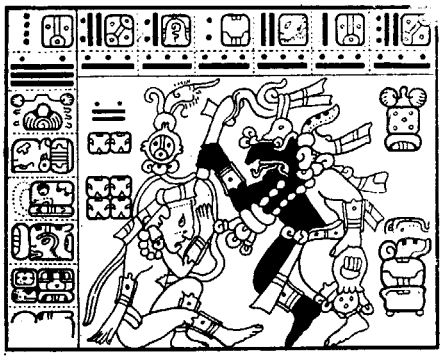
PERMUTATION TABLES INVOLVING A FEATURE OF NON-TRANSPOSABILITY

Umol-huun tah-tiyal

William Frederick

yetel

Elizebeth Smith Friedman



Lay ca-huunil kubenbil tech same.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a lo toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

30 April 1959

Paul S. Willard
Colonel, AGC
Adjutant General

~~*For Official Use Only*~~

Register No. 2

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

PERMUTATION TABLES INVOLVING A FEATURE OF NON-TRANSPOSABILITY

TECHNICAL PAPER

By

ABRAHAM SINKOV, Ph.D.
Junior Cryptanalyst

SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1934

CONTENTS

PERMUTATION TABLES INVOLVING A FEATURE OF NON-TRANSPOSABILITY

SECTION I

INTRODUCTORY REMARKS

1. **Permutation tables and the two-letter differential.**—Five-letter code words have been in use in telegraph, cable, and radio communication ever since 1903, when the International Telegraph Conference of London legitimatized their use. From the first, it was recognized that these words, being arbitrarily constructed, had to embody some features which would assist in their expeditious correction if garbled in transmission. The most important of these features was the adoption of a principle known as the "two-letter differential", that is, that all code words belonging to the same code must differ by a minimum of two letters, position being considered.

The early codes, therefore, embodied the two-letter differential but not in the most efficient way, as will now be explained.

In modern code books, the code groups are constructed by means of special charts or tables called by various names such as "Permutation Tables", "Garble Tables", "Error Detector Charts", and so on. We shall refer to them herein as "Permutation Tables." A sample table is shown in figure 1, reference to which will show how code words are constructed and how the two-letter difference is incorporated in the set of words coming from the table.

The table in figure 1 consists of three sections; that designated as section 1 gives the initial pair of letters of a code word, section 2 gives the central letter, and section 3 the final pair of letters. To construct a code word, select a letter from the column immediately to the left of section 1, for example, the letter B, and then proceed to the right on the same horizontal line and select a second letter, for example E, giving the initial pair of letters BE. Since the central letters are contained in section 2 we proceed down the column in which the E of BE is located, into section 2 and select a third letter, say I, giving the trigraph BEI. Then proceed to the right on the same horizontal line with I into section 3 and select a letter, say F, to be the final letter of the group. The fourth letter is that which appears at the head of the column in which F is located and is the letter A, giving the code word BEIAF. Now if this systematic procedure in constructing the groups is followed, all the groups will present a minimum two-letter difference. For example, with BEI as the root, the following groups can be constructed: BEIAF, BEIBE, BEICD, BEIDC, etc. These groups differ from one another by two letters.

If AEF is selected as a root, then the following groups may be constructed: AEFAB, AEFBA, AEFCZ, etc., all of which differ from the BEI groups and from one another by at least two letters. No matter what the initial pair of letters selected may be, the code groups will present a minimum two-letter difference if this procedure in construction is followed.

66342—34——2

2. **Difficulties arising as a result of transposition.**—In the usual type of code book, the code words are listed alphabetically accompanied by arbitrarily assigned meanings also arranged alphabetically. For example, the following arrangement might arise:

Code word	Meaning
BEIAF	He
BEIBE	—— can
BEICD	—— can be
BEIDC	—— can have
BEIEB	—— can not
BEIFA	—— can not be
BEIGZ	—— can not have
etc.	etc.

Now, while these words show a two-letter difference, in certain cases the distinction consists in a difference in the *identity* of the two letters (for example, BEIBE and BEIDC); in other cases, it consists merely in a difference in the *positions* occupied by the two letters (for example, BEIBE and BEIEB). Now one of the very common errors in code work is that occasioned by a psychological lapsus called by cryptographers "transposition", that is, a pair of letters exchange positions. Thus, if this psychological slip of the pencil takes place in the writing of the last two letters of the group BEIBE, for example, it produces the group BEIEB—which is not only a bona fide group in the same code, *but has exactly the opposite meaning.* Moreover, the context of the message might give no indication whatever of the presence of such a serious error. This same phenomenon of groups differing only by an interchange of two letters is also true with respect to the groups BEIAF and BEIFA, BEICD and BEIDC, et al. There are today many codes in which hundreds of such pairs are present, with meanings, and thus present many possibilities for serious error. In many cases messages may become unintelligible as the result of such an error.

It was not long before code compilers realized the danger of allowing the two-letter difference to consist, in many cases, merely of a difference in the position occupied by the two members of a pair of letters falling in homologous adjacent positions in a pair of groups. What was recognized as necessary to minimize the possibility of error is a type of table such that even when two letters exchanged positions, the resulting combination would still show at least a one-letter difference from all other groups in the code.

3. **Elimination of the transposition phenomenon.**—Methods for eliminating transpositions of adjacent letters were soon elaborated. These methods consisted in the use of a square having 27 cells on a side instead of 26, which is really equivalent to adding a new character to the alphabet and using a 27-letter sequence. An example of a table which was devised to suppress the adjacent transpositions is shown in figure 2.[1]

According to figure 2, no adjacent transpositions will yield bona fide groups. For example, given BEFAZ, there are no such groups as EBFAZ, BEAFZ, BFEAZ, or BEFZA.

But the transposition phenomenon is almost as frequent in the case of alternate letters as it is in that of adjacent letters, and when code compilers tried to eliminate *both* "adjacent" and "alternate" transpositions, they found themselves confronted with a difficult problem. Some of them came quite close to 90 percent efficiency in this regard, but failed to attain 100 percent

[1] Notes on Code Words, W. F. Friedman and C. J. Mendelsohn, American Math. Monthly, vol. 39 (1932), p. 408.

efficiency without sacrificing large numbers of code groups and thus reducing the size of the code. For example, in the case of figure 2, many instances of alternate transpositions can be found. Some of them are as follows:

ACBDE and BCADE
ABCDC and ADCBC
ADCAB and ADBAC

These represent single examples of each of three types, viz, transposition of the first and third letters, of the second and fourth, and of the third and fifth; many more can be found of each type.

4. **Summary of results.**—The method devised in this paper enables one to eliminate every possible transposition of two letters with a resulting very material increase in the accuracy of code communication. At the same time, it permits a sufficiently large number of groups to satisfy the demands of any existing code.

SECTION II

CONSTRUCTION OF TABLE

5. **Decimated sequences.**—The basic idea involved in this method is that of a decimated sequence. To illustrate, consider a given, ordered series of characters such as the digits from 1 to 9.

1 2 3 4 5 6 7 8 9

This sequence will be considered identical with any cyclic permutation of itself as e.g.

3 4 5 6 7 8 9 1 2 .

Suppose that, in the second sequence, every alternate character is chosen in order. Then the result

3 5 7 9 2 4 6 8 1

is said to have been obtained from either of the first two by the use of the decimation interval 2. The decimation interval 4 on the original sequence would have yielded

1 5 9 4 8 3 7 2 6 .

If the decimation interval has a factor in common with the number of characters in the sequence, the result, instead of being one complete cycle, will be a set of smaller sequences, each behaving as a unit. Such cases will not be considered in what follows. It is assumed *a priori* that every decimation interval used is relatively prime to the number of characters in the basic sequence; the basic sequence itself will be said to correspond to the decimation interval 1. (This concept is identical with the notion in group theory of the powers of a cyclic substitution.)

6. **Form of table.**—The permutation table which is now to be set up will have all its sequences derived by decimation from one basic sequence on n characters, the sequence itself being entirely arbitrary; the elimination of the various transposition types is accomplished by a proper choice of the decimation intervals. Corresponding to each type, an algebraic condition will be set up and any numbers which satisfy that condition will cause the removal of the particular transposition type. The basic sequence appears, in the table, to the left of section 1 and above section 3.

The six decimation intervals to be considered are as follows:

	Horizontal interval	Vertical interval
Section 1	a	b
Section 2	c	d
Section 3	e	f

Given these six numbers and the number of characters in the basic sequence, the complete table is readily constructed, since the basic sequence itself is entirely arbitrary and may involve any n characters in any order whatever. Of course, if the table is to be used for a code book

containing letter code groups, it would then be expected that the letters of the alphabet would be involved in the n characters of the basic sequence.

7. **Relations existing in sections of table.**—As a result of the use of decimated sequences, certain relations exist between the relative positions of particular letter combinations within the various sections of the table which make it possible to obtain the final conditions. In order to avoid unnecessary repetition, all these relations will be set down first and then the particular transposition types will be considered in turn.[1] The symbol θ will be used to mean "any letter"; θ_1 means "any letter in the first position", θ_2, "any letter in the second position", etc.

(a) SECTION 1. Two digraphs $\theta_1\theta_2$, $\theta_1\theta'_2$ having the same initial letter will be on the same row. If the number of columns between them is x, then the interval between θ_2 and θ'_2 in the basic sequence is ax.

Two digraphs chosen from the same column will differ in both their initial and final letters. Let them be represented by $\theta_1\theta_2$ and $\theta'_1\theta'_2$. Then, if the basic interval between θ_1 and θ'_1 is x, that between θ_2 and θ'_2 is bx.

Two digraphs $\theta_1\theta_2$ and $\theta'_1\theta_2$ whose final letters are the same will be in different columns and on different rows. If the number of rows between them, i.e., the basic interval between θ_1 and θ'_1 is x, then the number of columns separating $\theta_1\theta_2$ and $\theta'_1\theta_2$ is $-\frac{bx}{a}$.

(b) SECTION 2. Two letters on the same row and separated by x columns are cx letters apart in the basic sequence.

Two letters in the same column and separated by x rows are dx letters apart in the basic sequence.

Two like letters x rows apart are $-\frac{dx}{c}$ columns apart.

(c) SECTION 3. The results here are similar to those in section 1. Because of the position of the basic sequence, they are derivable from the results for section 1 by interchanging the words row and column, initial and final. The letters a and b must also be replaced by f and e respectively.

[1] The reasoning will be better appreciated by referring to fig. 3.

SECTION III

CONDITIONS FOR NON-TRANSPOSABILITY PROPERTIES

8. **Definition of transposition types.**—The following notation will make the exposition a bit simpler. Suppose two groups differ only in a transposition of the first and second letters as, e.g., RLOPN and LROPN. Then they will be designated as transpositions of type 1—2. Two groups differing only in the transposition of letters in the third and fifth positions will be said to be of type 3—5. In general, the notation "transpositions of type a—b" will mean an interchange of the letters in the a^{th} and b^{th} positions and "groups of type a—b" will mean groups differing only by a transposition of type a—b.

The various transposition types will now be taken up in order and the necessary condition obtained for each type.

9. **Condition for type 1—2.**—Groups of this type, such as $\theta_1\theta_2\theta_3\theta_4\theta_5$ and $\theta_2\theta_1\theta_3\theta_4\theta_5$, will arise whenever two digraphs $\theta_1\theta_2$ and $\theta_2\theta_1$ are found in the same column of section 1. If the basic interval between the initial letters θ_1 and θ_2 is x, the interval between the final letters is bx. In other words, there are x letters between θ_1 and θ_2, bx letters between θ_2 and θ_1. Hence,

$$x+bx\equiv 0 \pmod{n}$$
$$x(1+b)\equiv 0 \pmod{n}$$

Whenever this congruence has a solution for x, other than 0 or n, the permutation table will contain groups of type 1—2. A necessary and sufficient condition that there be no such solutions is that $1+b$ be relatively prime to n.

10. **Condition for type 2—3.**—Two such groups are of the form $\theta_1\theta_2\theta_3\theta_4\theta_5$, $\theta_1\theta_3\theta_2\theta_4\theta_5$. If the distance between θ_2 and θ_3 in section 1 is ax, that between θ_3 and θ_2 in section 2 is cx and therefore

$$x(a+c)\equiv 0 \pmod{n}$$

The elimination of this type requires $a+c$ to be prime to n.

11. **Condition for type 3—4.**—Let these groups be represented by $\theta_1\theta_2\theta_3\theta_4\theta_5$, $\theta_1\theta_2\theta_4\theta_3\theta_5$, and let the basic interval between θ_4 and θ_3 in section 3 be x. Then, the number of rows between $\theta_4\theta_5$ and $\theta_3\theta_5$ is $-\frac{ex}{f}$. This requires the basic interval between θ_3 and θ_4 in section 2 to be $-\frac{dex}{f}$. Hence,

$$x-\frac{dex}{f}\equiv 0 \pmod{n}$$

or

$$x\,(f-de)\equiv 0 \pmod{n}$$

As a result $f-de$ must be prime to n.

12. **Condition for type 4—5.**—The reasoning here is the same as for type 1—2 and leads to the condition

$$x\,(1+e)\equiv 0 \pmod{n}$$

13. **Conditions for remaining types.**—The reasoning for the remaining cases of types of the form a—b follows along the same lines. Although a bit more involved, it introduces nothing essentially new and, as a consequence, the results for these types will be set down without proof. The variable x may be eliminated in each case if it be required that its coefficient be relatively prime to n. On this basis, the necessary conditions for each type are that the expression given for it have no factor in common with n (nor must it be zero). It must also be remembered that each of the numbers a, b, c, d, e, f is prime to n.

Type	Expression
(1) 1—2	$1+b$
(2) 2—3	$a+c$
(3) 3—4	$f-ed$
(4) 4—5	$1+e$
(5) 1—3	$a-bc$
(6) 2—4	$aed+cf$
(7) 3—5	$d+f$
(8) 1—4	$ade-bcf$
(9) 2—5	$ad-cf$
(10) 1—5	$ad+bcf$

[redacted]able

[redacted]

(1) 1 + a
(2) b + d
(3) 1 + c
(4) a - bd
(5) c - bd

[redacted]

Any set of numbers which satisfies all foregoing 10 conditions [redacted] involving no transpositions of the types considered. If it is desired to eliminate only certain particular transposition types, it will be sufficient to consider only the conditions which apply to those types. The entire set cannot be satisfied unless certain restrictions are placed on the number n.

14. **Restrictions on number of letters in basic sequence.**—To get these restrictions, it should be observed that each of the expressions must be prime to any divisor of n. In other words, condition (2)

$$a+c\not\equiv 0 \pmod{n}$$

also implies

$$a+c\not\equiv 0 \pmod{d}$$

where d is any divisor of n. If now, we set

$$\begin{aligned} f &\equiv pd \\ a &\equiv qc \end{aligned} \qquad (p,q\not\equiv -1)$$

the four conditions involving b, viz, (1), (5), (8), and (10), reduce to

$$\begin{aligned} b &\not\equiv -1 && (1)\\ b &\not\equiv q && (5)\\ b &\not\equiv e\left(\frac{q}{p}\right) && (8)\\ b &\not\equiv -\left(\frac{q}{p}\right) && (10) \end{aligned}$$

The four numbers -1, q, $e\left(\frac{q}{p}\right)$, $-\left(\frac{q}{p}\right)$, can be shown to be all different, if the 10 equations of condition are satisfied. Consequently, there must be more than four numbers less than and prime to any factor of n, and as a result n can have no factor less than 7. For all numbers n divisible by no number less than 7, it is possible to satisfy all the conditions.

The table which has been designated figure 3 corresponds to the value $n=29$. It has been constructed according to the principles just described and involves no transpositions of any of the 10 types considered.[1] To check this statement is a simple task. The decimation intervals involved are as follows:

$$a=3$$
$$b=1$$
$$c=2$$
$$d=1$$
$$e=1$$
$$f=3$$

Substituting these values in the expressions of condition previously obtained shows that none of them is zero or has a factor in common with 29 and hence none of the 10 transposition types can arise. The set of numbers used here for decimation intervals represents only one of infinitely many possibilities; it requires very little effort to find other sets which will satisfy all the necessary conditions. It may be of interest to observe in this connection that a set of decimation intervals which is valid for any one prime number n is also valid for any other prime number which exceeds n.

The table for $n=29$ is the smallest one that can be made to embody all the features discussed here and which will at the same time involve all the letters of the alphabet in the basic sequence. For such a table the maximum number of groups possible is 409,711. The greatest possible number of two-letter difference groups obtainable is 456,976. In other words, the process of suppressing all 10 transposition types involving two letters has caused a loss of only 10.3 percent of the total available number of groups.

Although the principles involved in this paper have been applied to the case of five-letter code words, it is patent that they are applicable to similar problems involving combinations of any number of letters or symbols. The importance of the number 5 lies in the fact that present-day code communication is almost entirely carried on in five-letter groups.

[1] In fig. 3 the three additional characters "1", "2", "3", serve merely as "fillers" occupying the indicated extra cells required by the conditions. When such a table is actually used for constructing the code words, these cells would merely be left blank or would be occupied by dots, as in fig. 2.

SECTION 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

SECTION 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
2	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
3	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
4	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
5	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
6	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
7	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
8	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
9	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
10	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
11	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
12	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
13	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
14	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
15	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
16	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
17	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
18	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
19	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
20	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
21	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
22	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
23	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
24	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
25	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
26	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

SECTION 3

FIGURE 1

Section 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
.	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B
4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C
5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D
6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E
7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F
8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G
9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H
10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I
11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J
12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K
13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L
14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M
15	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N
16	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
17	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
18	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
19	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
20	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
21	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
22	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
23	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
24	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
25	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
26	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
27	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Section 2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
2	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
4	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
5	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
6	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
7	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
8	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
9	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
10	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
11	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
12	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
13	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L	M
16	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K	L
17	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J	K
18	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I	J
19	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H	I
20	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G	H
21	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F	G
22	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E	F
23	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D	E
24	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C	D
25	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B	C
26	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A	B
27	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	A

Section 3

Figure 2

SECTION 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2
2	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3
3	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A
4	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B
5	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C
6	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D
7	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E
8	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F
9	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G
10	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H
11	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I
12	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J
13	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K
14	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L
15	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M
16	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N
17	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O
18	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P
19	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q
20	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R
21	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S
22	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T
23	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U
24	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V
25	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W
26	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X
27	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y
28	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1	3	B	D	F	H	J	L	N	P	R	T	V	X	Z
29	3	B	D	F	H	J	L	N	P	R	T	V	X	Z	2	A	C	E	G	I	K	M	O	Q	S	U	W	Y	1

Note: See footnote 1, page 8.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3
2	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C
3	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F
4	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I
5	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L
6	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
7	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
8	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
9	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
10	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1
11	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A
12	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D
13	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G
14	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J
15	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M
16	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
18	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
19	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
20	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2
21	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B
22	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E
23	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H
24	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K
25	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N
26	R	S	T	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
27	U	V	W	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
28	X	Y	Z	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
29	1	2	3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z