Two Applications of a Hamming Code

Andy Liu

Andy Liu (al3@ualberta.ca) has a doctorate in mathematics and a graduate diploma in elementary education. His research interest spans combinatorics, geometry, mathematics recreation, and mathematics education. He is at present on the Board of Governors of the MAA, and serves as co-editor of the Problem Corner in *Math Horizons*. He was the Deputy Leader of the USA IMO team from 1981 to 1984, and won a Tepper Haimo Award in 2004.

Dedicated to the memory of
Murray Seymour Klamkin (1921–2004)

Alice wants to send messages to Michael. They have a transmitter that sends fifteen binary digits at a time. Unfortunately, their messages may be intercepted by a saboteur who is able to change at most one of the fifteen bits from a 0 into a 1, or vice versa. When this happens, it may have serious consequences. Alice and Michael would like to know whether a message has been tampered with, and, if possible, what the original message was.

Alice and Michael devise a communication scheme based on set theory. To send her binary message, Alice prepares the chart as shown below.

A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q
a	a	a	a		a	a	a				a			
b	b	b		b	b			b	b			b		
c	c		c	c		c		c		c			c	
d		d	d	d			d		d	d				d

The columns are the $2^4 - 1 = 15$ nonempty subsets of the four-element set $\{a, b, c, d\}$. The 4 one-element subsets are separated from the others by a vertical line. The message is sent 11 digits at a time, entered on the bottom line under the columns labelled A, B, C, D, E, F, G, H, J, K, and L. The 4 digits under M, N, P, and Q are added for protection. They are chosen so that

$$A + B + C + D + F + G + H + M \equiv 0 \pmod 2, \tag{1}$$

$$A + B + C + E + F + J + K + N \equiv 0 \pmod 2, \tag{2}$$

$$A + B + D + E + G + J + L + P \equiv 0 \pmod 2, \tag{3}$$

$$A + C + D + E + H + K + L + Q \equiv 0 \pmod 2. \tag{4}$$

Note that the eight columns involved in (1) are those containing the letter a. Similarly, the eight columns involved in (2), (3), and (4) are those containing the letters b, c, and d, respectively.

For example, suppose the first 11 digits of Alice's message are 10111100011. The protection digits are computed using (1) to (4). We have

$$M \equiv A + B + C + D + F + G + H \equiv 0 \pmod 2,$$
$$N \equiv A + B + C + E + F + J + K \equiv 1 \pmod 2,$$
$$P \equiv A + B + D + E + G + J + L \equiv 0 \pmod 2,$$
$$Q \equiv A + C + D + E + H + K + L \equiv 0 \pmod 2.$$

Suppose Michael receives the message shown in the following chart.

A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q
a	a	a	a		a	a	a				a			
b	b	b		b	b			b	b			b		
c	c		c	c		c		c		c			c	
d		d	d	d			d		d	d				d
1	0	1	1	1	0	0	0	0	1	1	0	1	0	0

He checks the four congruences, and finds that (3) and (4) hold while (1) and (2) fail. Since the error affects a and b but not c or d, it must occur under the subset $\{a, b\}$, so that the digit under F is wrong.

A team competition

When he finally deciphers Alice's entire message, Michael learns that the two of them, along with thirteen of their friends, are entered in a team competition organized by a certain hi-tech company. They will be put respectively into rooms A to Q (there are no rooms I and O). Each room is considered to be in one of two states, 0 or 1, assigned completely at random. Once they are isolated in their rooms, the team members will be informed of the state of each room except their own. Simultaneously, each must either pass, or declare the state of her or his room. They will have no further communication with their teammates, and are not aware of the action taken by any of them. If everybody passes, the team will be disqualified. If at least one declaration is incorrect, the team will also be disqualified. On the other hand, if there is at least one declaration, and all declarations are correct, the team wins a prize.

Alice, Michael and friends are given a short time to come up with some strategy. For instance, they could designate Alice as the guesser and have everyone else pass. The probability of winning a prize would then be $\frac{1}{2}$. However, they would like to do better. Alice and Michael recall the commuication scheme they have used, and come up with the following strategy.

We first give an illustration. Suppose Alice is in Room G and Michael is in Room N, and the actual states are as shown in the diagram below.

Rooms	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q
Communi-	a	a	a	a		a	a	a				a			
cation	b	b	b		b	b			b	b			b		
Scheme	c	c		c	c		c		c		c			c	
Set-up	d		d	d	d			d		d	d				d
Actual States	0	1	1	1	0	1	1	0	0	1	1	0	0	1	0
Alice	0	1	1	1	0	1	?	0	0	1	1	0	0	1	0
Michael	0	1	1	1	0	1	1	0	0	1	1	0	?	1	0

Alice checks that all of congruences (1) to (4) will hold if the state of her room is 0. So Alice will declare the opposite state 1. Michael checks that congruence (1) cannot hold regardless of whether the state of his room is 0 or 1. So Michael passes.

This illustrates how things work in general. A team member declares if, and only if, the state of her or his room can be chosen to fix everything in the communication scheme, but the opposite state is declared. If the original set-up contains no errors when treated as a communicated message, every team member will make an incorrect declaration. If the original set-up contains an error, only the team member in the room corresponding to where the error occurs will declare, and the declaration will be correct.

Recall that, in the communication scheme, the 4 protection digits are uniquely determined by the 11 message digits. Of the $2^4 = 16$ possible sequences for those 4 digits, only the one obtained from computations using (1) to (4) contains no errors. Hence $\frac{15}{16}$ of the time, the original set-up contains an error. It follows that the probability of winning a prize is $\frac{15}{16}$.

A magic trick

To celebrate their success in the team competition, the fifteen friends have a party, during which Alice and Michael perform a magic trick.

While Michael is out of the room, the audience chooses one of the sixteen letters from A to R inclusive, but excluding I and O. Then the audience places sixteen coins in a row, arbitrarily deciding whether each should be heads or tails. Alice turns over exactly one coin, and leaves the room while Michael is brought back in. By looking at the coins and without knowing which one Alice has turned over, Michael determines the letter chosen by the audience.

Let us give an illustration. We use 0 to stand for a coin which is heads and 1 for a coin tails. Suppose the audience chooses the letter K and places the coins as shown in the chart below, with an extra column for the empty subset of $\{a, b, c, d\}$.

Letters	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R
Communi-	a	a	a	a		a	a	a				a				
cation	b	b	b		b	b			b	b			b			
Scheme	c	c		c	c		c		c		c			c		
Set-up	d		d	d	d			d		d	d				d	
Coins	1	0	1	1	1	0	0	0	0	1	1	0	1	0	0	1

Checking the four congruences, Alice finds that (1) and (2) fail while (3) and (4) hold. Since the letters under column K are b and d, Alice wants (2) and (4) to fail while (1) and (3) hold. So she has to adjust (1) and (4). This can be done with the flipping of only one coin, which must be under the column associated with the subset $\{a, d\}$. Hence she changes the 0 under column H to 1. When Michael returns, he checks the four congruences, and finds that (1) and (3) hold while (2) and (4) fail. This means that the number chosen by the audience is the one in the column associated with the subset $\{b, d\}$, namely K.

Concluding remarks

The communication device of Alice and Michael is a special case of the famous Hamming Code. For the description of the general case, see [**4**] and [**3**]. The set-theoretic

presentation is given in [**1**] and [**5**]. For the presentation of a smaller case using Venn diagrams, see [**2**].

The team competition application is given in [**6**] as the problem titled *Crowning the Minotaur*. The Hamming code is mentioned in the solution. It has also come to be known as the Hat Problem. The magic trick application is based on a problem in the Fall Round of the 2007 International Mathematics Tournament of the Towns. The official solution did not involve the Hamming code.

If the number of coins in the magic trick is not a power of two, the strategy will not work. However, could there be some other strategy that work for, say, ten coins?

The answer is no. There are altogether $2^{10} = 1024$ different arrangements of the ten coins. Each of them signals to Michael one of the letters from A to K inclusive, excluding I. Since $1024 \div 10 < 103$, some letter is signaled by at most 102 arrangements. By turning over exactly one coin, each of the 1024 arrangements must be convertible to one of these 102. However, 102 targets can receive at most $102 \times 10 = 1020$ conversions, and we have a contradiction. The same reasoning shows that no other protocol can work if the number of coins is different from a power of two.

References

1. N. Alon and A. Liu, An application of set theory to coding theory, *Math. Mag.* **62** (1989) 233–237.
2. COMAP, *For All Practical Purposes*, W. H. Freeman, New York, 2006.
3. M. J. E. Golay, Notes on digital coding, *Proc. I.E.E.E.* **37** (1949) 657.
4. R. W. Hamming, Error detecting and correcting codes, *Bell System Tech. J.* **29** (1950) 147–160.
5. A. Liu, In search of a missing link: A case study in error-correcting codes, this JOURNAL **32** (2001) 343–347.
6. D. E. Shasha, *Puzzling Adventures*, W. W. Norton, New York, 2005.

You will find his picture in every book on the history of mathematics, an old saintly figure with a long beard and a wise expression in his eyes. But who was this most revered person? The truth is, we don't know. Pythagoras is one of the most mysterious figures in history; the little we do know about him may be more fiction than fact, written by historians who lived hundreds of years later. So everything you read about him—and most certainly the image on that bearded portrait—must be taken with a grain of salt.

Ali Maor, *The Pythagorean Theorem*, p. 208