Introduction to Codes and Algebraic Combinatorics

Special Lecture at Ateneo de Manila University

Hiroshi Suzuki
Division of Natural Sciences
International Christian University
Mitaka, Tokyo 8585, JAPAN

December 4, 2002

1 Introduction

Magandan hapon! I have to make an excuse first. I made a few slides but I will mainly use the white board as I like the speed to share mathematics with it. Please tolerate my poor hand writing as well.

1.1 Error Correcting Codes

Claude Elwood Shannon (1916.4.30-2001.2.24) Can you identify who this person is?[1] He is Claude Elwood Shannon, “the mathematician who laid the foundation of modern information theory while working at Bell Labs in the 1940s.” “Claude Elwood Shannon is considered as the founding father of electronic communications age.” “He graduated from the University of Michigan in 1936 with bachelor’s degrees in mathematics and electrical engineering. In 1940 he earned both a master’s degree in electrical engineering and a Ph.D. in mathematics from the Massachusetts Institute of Technology (MIT).”

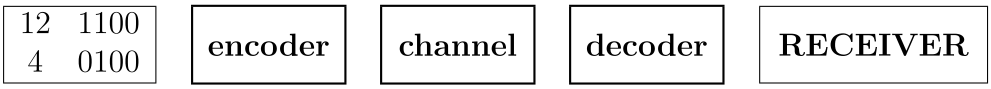
He set the foundation of the theory of error correcting codes in a memorable paper:

[1] 1st slide: a picture and quotes of Claude Elwood Shannon are taken from http://www.bell-labs.com/news/2001/february/26/1.html

[S] Claude E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal **27** (1948), 379–423, 623–656.

Error detecting to error correcting: Let me explain what an error correcting code is.

We want to transmit some information through a channel. Suppose we want to send today's date by two numbers 12 and 4. We first change this into binary expression, 1100 and 0100. If these combinations of 1's and 0's reach the receiver without noise, there is no problem. Suppose some noise may change some of the 1's to 0's and some of the 0's to 1's. We want to add extra information to the original data by an encoder so that we can recover the original information by an decoder even if some changes may occur. We want not only to detect the error but correct the error. One way to do it is to send the same information many times. Then even if some bits may change by noise, we can recover the original message by majority rule.



The most attractive point of coding theory is that we can apply various mathematical tools to solve practical problems.

Algebra, linear algebra, number theory, algebraic geometry, statistics, computer assisted enumeration, engineering, etc., etc., ...

Error correcting codes have many applications in communication channel, compact disk (CD), Bar Code, or RAID (Redundant Array of Independent Disks). For example, even if you put a scar by a knife on the surface of a music CD, you can listen to the music without any noise. It is because so-called 2-error correcting Reed-Solomon code is used to record the information on a CD.

Why I like error correcting codes: With the theory of cryptography [for security] coding theory is one of the most important fields in information science and information mathematics. I do not know much about cryptography, but it seems to be a very interesting subject as well. Some people say if you want to make money as a mathematician, cryptography is the best field you should invest.

I introduced Shannon. He is not only the father of information theory, and error correcting codes but it is said "another example is Shannon's 1949 paper entitled Communication Theory of Secrecy Systems. This work is now generally credited with transforming cryptography from an art to a science."

So he set foundation of these two important fields in information science and mathematics, very rare examples of useful mathematics. Did he want to make money? In the same article:

> Shannon was renowned for his eclectic interests and capabilities. A favorite story describes him juggling while riding a unicycle down the halls of Bell Labs. He designed and built chess-playing, maze-solving, juggling and mind-reading machines. These activities bear out Shannon's claim that he was more motivated by curiosity than usefulness.
>
> In his words "I just wondered how things were put together."

Besides intellectual curiosity, let me explain why I personally like "error correcting code" more than cryptography.

As a human being, we cannot avoid making mistakes. But we do not want someone to point out our errors or mistakes. If someone not only detects but corrects our errors and covers up our flaws in our daily life before we even notice that we made a mistake, it is wonderful, though we should be humble. We also know that if we pursuit efficiency only, we cannot live spiritually rich life, and it is something redundant that gives us 'healing' and richness in life.

Now I would like to come back to my business to introduce codes and the theory behind.

1.2 Hamming Code $[7, 4, 3]$:

As some of you may know, there are various types of error correcting codes. What we focus today is so called block codes. Those are codes that we encode and decode as a block of same length. First let us see how it works.

We need two matrices.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad H^T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

We send a binary data of length four.

Let us send $(12, 4)$ or 12 and 4 in binary representation. So they become $(1100), (0100)$. Assume that there may be some noise to change 1 to 0 or 0 to 1. If we send these words only, there is no way to recover the information. So we add some extra. Instead of sending a we send $a \cdot G$. (See the table below.) We use matrix multiplication under the following convention.

Computation in $F = \{0, 1\}$:

$$0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1,\ 1 + 1 = 0 \tag{1}$$

$$0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0,\ 1 \cdot 1 = 1 \tag{2}$$

$$\begin{aligned} 12 &: (1100) \cdot G = (1100110) \\ 4 &: (0100) \cdot G = (0100101) \end{aligned}$$

Suppose there was some noise and it changed a part. As a result we got x. Then we compute $x \cdot H^T$. The decimal number of it tells where the error occurred.

For example if the fourth digit of (1100110) changed from 0 to 1 and (1101110) is received. Since $(1101110)H^T = (100)$ and the decimal number of (100) is 4, it indicates that the error occurred in the fourth digit. Hence we can recover (1100110) by changing the fourth digit from 1 to 0. For the second, suppose we received (0100100). Since $(0100100)H^T = (111)$, it suggests that the error occurred in the seventh digit. We recover the original information (0100101).

	a				aG							wt
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	1	1	1	1	4
2	0	0	1	0	0	0	1	0	1	1	0	3
3	0	0	1	1	0	0	1	1	0	0	1	3
4	0	1	0	0	0	1	0	0	1	0	1	3
5	0	1	0	1	0	1	0	1	0	1	0	3
6	0	1	1	0	0	1	1	0	0	1	1	4
7	0	1	1	1	0	1	1	1	1	0	0	4
8	1	0	0	0	1	0	0	0	0	1	1	3
9	1	0	0	1	1	0	0	1	1	0	0	3
A	1	0	1	0	1	0	1	0	1	0	1	4
B	1	0	1	1	1	0	1	1	0	1	0	4
C	1	1	0	0	1	1	0	0	1	1	0	4
D	1	1	0	1	1	1	0	1	0	0	1	4
E	1	1	1	0	1	1	1	0	0	0	0	3
F	1	1	1	1	1	1	1	1	1	1	1	7

Let us think why it worked.

$$\begin{array}{rcl} C & = & \{x \cdot G \mid x \in F^4\} \\ & = & \left\{ \begin{array}{llll} (0000000), & (0001111), & (0010110), & (0011001), \\ (0100101), & (0101010), & (0110011), & (0111100), \\ (1000011), & (1001100), & (1010101), & (1011010), \\ (1100110), & (1101001), & (1110000), & (1111111) \end{array} \right\} \subset V = F^7 \end{array}$$

Then we find

$$c + c' \in C \quad \text{for every } c, c' \in C \tag{3}$$

It is clear as we multiplied the vector in the data set F^4 by the matrix G. If we are allowed to use terminology in algebra. C is a subgroup of V, or if we look at V as a vector space over F, i.e., the field with two elements, the image of a linear mapping defined by the matrix G is a linear subspace. We call these codes binary linear codes of length 7.

Moreover, let us observe that we have

$$G \cdot H^T = O,$$

where O denotes the zero matrix (of size 4×3 in this case). When we send a (a binary information of length 4), we compute $c = a \cdot G$ and send this word of length 7 instead. Hence,

$$c \cdot H^T = a \cdot G \cdot H^T = a \cdot O = (000) \quad \text{for every } c \in C \tag{4}$$

Let

$$\begin{array}{rcl} e_1 & = & (1000000) \\ e_2 & = & (0100000) \\ e_3 & = & (0010000) \\ e_4 & = & (0001000) \\ e_5 & = & (0000100) \\ e_6 & = & (0000010) \\ e_7 & = & (0000001). \end{array}$$

Let $c \in C$. If there is an error in ith bit (or position), then we have $c + e_i$. Then by (4) we have $(c+e_i) \cdot H^T = e_i \cdot H^T$, which is nothing but the ith column of H^T. But the ith column of H^T is the binary expression of i. We can tell the position the error occurred. Hence we can recover the correct information as far as the error occurred at only one place. Then what happens if no error occurred? In that case we conclude that the error occurred at 0th position because of (4),

For $x, y \in V = F^7$, let

$$\partial(x, y) = \text{number of distinct entries.}$$

$\partial(x, y)$ is called the (Hamming) distance of two vectors in V. Then

$$\partial(x, y) = \text{the number of nonzero coordinates of } x - y. \tag{5}$$

The number of nonzero coordinates of a vector x is also called the (Hamming) weight $\mathrm{wt}(x)$. Let $c, c' \in C$ with $c \neq c'$. Then $c - c'$ is a nonzero member of C by (3). Note that in V, $c - c' = c + c'$ by (1). From the table, $\partial(x - y, 0) \geq 3$. Hence every pair of code words in C is at least distance 3 apart each other. So even if the code word c changed at one place, still we can tell what the code originally was, because that is the only code word at distance 1.

Hence the redundancy corrects errors. In daily conversation, by natural language, we can understand the conversation even if the listener cannot catch every word the speaker speaks. With this redundancy we can communicate the core of the message. Since English is not my native tongue, I can never be perfect in my language. But I hope you can understand my message. It is only possible as far as the number of errors does not exceed the capacity of the error correction.

Recently, it is reported that the analysis of the gene, or the DNA of human beings is fully developed and we can tell the genetic information in DNA. And as you mostly know that the major part of the DNA is called intron which does not carry genetic information. I understand that when DNA replicates and produce a so-called messenger RNA which has full information to generate a molecule of a protein, this part is not used. On the other hand in the process of replication, it often makes mistakes by skipping some of the parts, but some parts of intron send signals to repair such error to produce exact mate of the part of DNA. We do not have full understanding of this error correction method in our body but I believe that some parts of intron have very important role for repair of the flaw in the process. It is also said that the number of genes of advanced species does not differ much from primitive ones, however, the quantity of intron is very much different. So it is understood that this part was formed in the process of evolution in the history of trials and errors. But I think that there may be other meaning of this supposedly unnecessary part of DNA to work as an error correction or something else. I am not a specialist in this subject, so please ask your friends in Biology for details to enrich your understanding of life.

Goal of Coding Theory:

- Invent useful codes, or invent efficient decoding systems.
- Construct good codes which are close to so-called theoretical bound.
- Study mathematical condition around the good codes.

We need to define what we mean by 'good' codes. Roughly speaking, for a code of length n, we want to maximize the number of code words $|C|$ keeping the capacity of error correction e large. In the following we will see some specific descriptions of good codes and the induced combinatorial structures.

2 Combinatorial Structures of Codes

2.1 Perfect Code:

Let $C \subset F^n$. The minimum distance $d(C)$ of C is

$$d = d(C) = \min\{\partial(c, c') \mid c, c' \in C,\ c \neq c'\}.$$

Assume that C is an e-error correcting code of length n. By e-error correcting, we mean it has capacity to correct up to e errors in a code word. In order to guarantee C to be e-error correcting, we need $d(C) \geq 2e+1$. Let $B_e(c)$ denote the ball of radius e centered at a code word $c \in C$, that is the set of vectors in F^n at distance at most e from c. If $c \neq c'$ are code words, then $\partial(c, c') \geq 2e+1$ and $B_e(c) \cap B_e(c') = \emptyset$. Hence

$$\bigcup_{c \in C} B_e(c) \subset V \quad \text{(disjoint).} \tag{6}$$

Let $c = (c_1, c_2, \ldots, c_n) \in C$. Then the distance from x to c is 1 if and only if x is different from c in exactly one coordinate. So there are exactly n such vectors. There are ${}_nC_2$ vectors which are at distance 2 from c, and so on. We can compute the cardinality of $B_e(c)$ and it is $\sum_{i=0}^{e} {}_nC_i$. So by (6) we have

$$|C| \cdot \sum_{i=0}^{e} {}_nC_i \leq |F^n| = 2^n.$$

In our example, $|C| = 16 = 2^4$, $n = 7$, $e = 1$, and $d = 3$. So we have

$$2^4 \cdot \sum_{i=0}^{1} {}_7C_i = 2^4(1+7) = 2^7 = |F^7|$$

In this case, it is not an inequality but an equality they satisfy. That means we must have equality in (6) and that if we collect all vectors which are at distance $0, 1, \ldots, e$ from codes in C, we have all vectors in F^n. This is a very special case. Since it gives a perfect partition of the underlying space V, it is called a *perfect code.* The example we studied, i.e, Hamming [7,4,3] code, is an example of a perfect code.

A subset C of $V = F^n$ satisfying (3) becomes a linear subspace of V. Let $k = \dim C$. Such a code is called a binary linear code of length n, dimension k, or $[n, k, d]$ code if $d = d(C)$ is the minimum distance.

Binary Golay Code:

Let us introduce another example.

$$G = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&1&1&1&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1
\end{bmatrix}$$

The following is the square elements modulo 11.

$$\begin{aligned}
\{m^2 \mid m \in \boldsymbol{Z}_{11}\} &= \{0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 5,\ 5^2 = 3,\ 6^2 = 3, \\
&\quad\ 7^2 = 5,\ 8^2 = 9,\ 9^2 = 4,\ 10^2 = 1\} \\
&= \{0\} \cup \{1, 3, 4, 5, 9\}.
\end{aligned}$$

The matrix above is made using this set. Can you tell how this matrix is made by the set $\{0, 1, 3, 4, 5, 9\}$? The code using this matrix G is called the Binary Golay Code [23, 12, 7]. This is 3-error correcting. That means that suppose errors occur somewhere in a code word of length 23, if the number of errors is at most 3 then we can recover the original code word. Isn't it nice. This is also a perfect code.

$$2^{12}(1 + {}_{23}C_1 + {}_{23}C_2 + {}_{23}C_3) = 2^{12}(1 + 23 + 253 + 1771) = 2^{12} \cdot 2^{11} = 2^{23}$$

Theorem Nontrivial binary e-error correcting perfect code ($e \geq 1$) is either the Binary Golay Code or has the same parameter as the Hamming code $[2^m - 1, 2^m - m - 1, 3]$.

We need to explain what nontrivial means. The code consisting of the zero vector $(000\cdots 0)$ or the code consisting of the zero and $(111\cdots 1)$ are trivial ones. These are not very interesting so the theorem states only nontrivial ones.

Perfect code is a very good code but Theorem says that there are not so many perfect codes. Next we pick one of the good properties of perfect codes. This property is not strong enough to characterize perfect codes but there are many codes which satisfy this property.

2.2 Completely Regular Codes

In order to introduce this property, we first generalize the definition of codes, and define it as a subset of a graph.

Let $\Gamma = (X, E)$ be a graph with vertex set X and edge set E. E is a set of unordered pairs of X. Two vertices $x, y \in X$ are said to be adjacent if $(x, y) \in E$. For $x, y \in X$ the distance $\partial(x, y)$ denotes the minimal length of walks connecting x and y by a sequence of edges. For example, if $(x, y) \in E$, $\partial(x, y) = 1$, and $\partial(x, z) \leq 2$ if $(x, y), (y, z) \in E$. If the distance is always finite, in other words, if there is always a walk connecting two vertices, the graph is said to be connected. For a connected graph the diameter is the largest distance of vertices,

$$D = \max\{\partial(x, y) \mid x, y \in X\}.$$

$H(D, 2)$**:** As an example we define a Hamming graph $H(D, 2)$. Let $F = \{0, 1\}$ be as before. The vertex set of the Hamming graph $\Gamma = (X, E)$ is $X = F^D$, and the edge set is defined as follows.

$$E = \{(x, y) \mid x, y \in F^D,\ x \text{ and } y \text{ differ at exactly one coordinate}\}$$

Then it is not difficult to show that

$$\partial(x, y) = \partial(x - y, 0) = \text{the number of nonzero coordinates of } x - y. \quad (7)$$

See (5).

We consider a subset in a connected graph. Let C be a subset of X. In general, we call a subset of a graph a code.

$$w(C) = \max\{\partial(x, y) \mid x, y \in C\}$$

is called the width of C. For a vertex $x \in X$,

$$\partial(x, C) = \min\{\partial(x, y) \mid y \in C\}.$$

Let

$$C_i = \{x \in X \mid \partial(x, C) = i\}.$$

Then $C = C_0$ and we have a partition

$$X = C_0 \cup C_1 \cup \cdots \cup C_t,$$

where $t = t(C) = \max\{\partial(x, C) \,||\, x \in X\}$, which is called the covering radius.

Definition 1 C is a *completely regular code*[2] if the number

$$b_{i,j} = b_{i,j}(x) = |\{z \in C_i \mid \partial(z, x) = 1\}|$$

is independent of $x \in C_j$ for every i, j.

It is easy to see that if $b_{i,j} = 0$ if $|i - j| > 1$. The following square matrix of size $t + 1$ is called the intersection matrix of C.

$$B(\Gamma, C) = [b_{i,j}] = \begin{bmatrix} b_{0,0} & b_{0,1} & & & & \\ b_{1,0} & b_{1,1} & b_{1,2} & & \text{\Huge 0} & \\ & b_{2,1} & b_{2,2} & \cdots & & \\ & & \cdots\cdots & & & \\ & & & \cdots & b_{t-1,t-1} & b_{t-1,t} \\ \text{\Huge 0} & & & & b_{t,t-1} & b_{t,t} \end{bmatrix}$$

In the first example, we were considering a graph $H(7, 3)$ and a code C of cardinality 16. It is easy to check that C is completely regular. $F^7 = C_0 \cup C_1$, where $C = C_0$. Hence in this case $t(C) = 1$ and $w(C) = 7$.

$$B(\Gamma, C) = \begin{bmatrix} 0 & 1 \\ 7 & 6 \end{bmatrix}$$

It is known that every perfect code is completely regular. Hence the Binary Golay code we introduced above is also a completely regular code. The following is the intersection matrix of the Binary Golay Code. Can you compute the entries of it by yourself?

$$B(\Gamma, C) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 23 & 0 & 2 & 0 \\ 0 & 22 & 0 & 3 \\ 0 & 0 & 23 & 20 \end{bmatrix}$$

Perfect codes have many more interesting connections to completely regular codes. Please study some of the literatures and articles given at the end.

[2] The definition of completely regular codes here is not standard. This definition coincides with the standard definition if Γ is distance-regular. See [2, 10, 11].

2.3 Completely Regular Codes in $H(7,2)$

Let us determine completely regular codes C in $H(7,2)$ with small number of vertices.

$|C| = 1$: If $|C| = 1$. Then it is always completely regular with the following intersection matrix.

$$B(\Gamma, C) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

It is known that if every set consisting of a single vertex is completely regular then the underlying graph is either distance-regular or distance-biregular. We will not get into the detail but distance-regular graphs and distance-biregular graphs are graphs with very high combinatorial regularities. $H(D,2)$ and all Platonic solids are examples of distance-regular graphs.

$|C| = 2$: Let $C = \{x, y\}$. Suppose $\partial(x,y) = w(C) = \ell$. We want to show that either $\ell = 1$ or 7. Suppose $\ell = 2$. Then it is not difficult to show that there exist vertices z and z' with the following conditions.

$$\partial(x,z) = \partial(z,y) = \partial(y,z') = 1,\ \partial(x,z') = 3.$$

Then $b_{0,1}(z) = 2 \neq 1 = b_{0,1}(z')$. Hence it is not completely regular. The other cases can be treated similarly.

On the other hand if $\ell = w(C) = 1$, then $t(C) = 6$ and it is always completely regular.

$$B(\Gamma, C) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 5 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

If $\ell = w(C) = 7$, then $t(C) = 3$ and again it is always completely regular.

$$B(\Gamma, C) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 7 & 0 & 2 & 0 \\ 0 & 6 & 0 & 3 \\ 0 & 0 & 5 & 4 \end{bmatrix}$$

Can you go further to determine all completely regular codes in $H(7,2)$?

3 Problems

We close this lecture by giving two problems to determine special types of completely regular codes in $H(D,2)$. $|C| = 2$ with $w(C) = 1$ satisfies the condition in Problem 1. The Binary Golay Code is an example of the second one. We are assuming $|C| > 2$ as the example similar to the case $|C| = 2$ with $w(C) = 7$ can be constructed easily. I believe these are open problems. That means no one knows the solution yet. Do you want to challenge?

Problem 1 Determine all completely regular codes C in $H(D,2)$ such that

$$D = w(C) + t(C).$$

Problem 2 Determine all completely regular codes C in $H(D,2)$ such that $d(C) \geq 7$ with $|C| > 2$.

Thank you very much.

4 Questionnaire

Q1 What impressed you most about mathematics or about other aspects of your life?

Q2 Why do you study math? Why do they (including non-science major students) need to study math at high school or college?

Q3 What do you dream about accomplishing in your life? What do you want to pass on to the next generation?

Q4 Comments on the lecture.

The questionnaire with these questions are distributed and collected at the lecture. The responses are uploaded at the following site.

http://science.icu.ac.jp/˜hsuzuki/ateneo2002/

I will delete it upon request. Please send an email to hsuzuki@icu.ac.jp if any inconvenience may arise.

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, California, 1984.

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer Verlag, Berlin, Heidelberg, 1989.

[3] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups, Third Edition*, Springer, New York (1998).

[4] P. Delsarte, An algebraic approach to the association schemes of coding theory, Phillips Research Reports Suppl. 10 (1973).

[5] M. A. Fiol and E. Garriga, On the algebraic theory of pseudo-distance-regularity around a set, Linear Algebra Appl. 298 (1999), 115-141.

[6] M. A. Fiol and E. Garriga, An algebraic characterization of completely regular codes in distance-regular graphs, SIAM J. Discrete Math. 15 (2001/02), 1-13.

[7] C. D. Godsil, *Algebraic Combinatorics*, Chapman and Hall, Inc., New York, 1993.

[8] M. Giudice and C. E. Praeger, Completely transitive codes in Hamming graphs, European J. Combin. 20 (1999), 647-661.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publ. Co., Amsterdam (1977).

[10] A. Neumaier, Completely regular codes, Discrete Math., 106/107 (1992), 353-360.

[11] H. Suzuki, The Terwilliger algebra associated with a set of vertices in a distance-regular graph, preprint.