

Lecture of January 12th, 2007

Scribe: Frank Kschischang

1 Error-Correcting Capability of a Code

The following theorem relates the minimum Hamming distance of a code C to the number of errors guaranteed to be correctable by the code.

★ **Theorem:** If $2t < d_{\min}(\mathbf{C})$, then every error pattern of t or fewer errors is corrected by a minimum distance decoder for \mathbf{C} .

Proof: Let \mathbf{C} be a block code of length n over alphabet A . Suppose $x \in \mathbf{C}$ is sent and that $y \in A^n$ is received, and suppose that $d(x, y) = t$. Let $w \in \mathbf{C}$ be a codeword *other than* x . The decoder will make an error if it returns w instead of x . Since x and w are codewords, we have $d_{\min}(\mathbf{C}) \leq d(x, w)$. By the triangle inequality, we have $d(x, w) \leq d(x, y) + d(y, w) = t + d(y, w)$. Thus, $d(y, w) \geq d_{\min}(\mathbf{C}) - t$. If $d_{\min}(\mathbf{C}) > 2t$, then $d(y, w) > t$, and so the minimum distance decoder will not return w instead of x . ■

If \mathbf{C} is a given code of minimum distance $d_{\min}(\mathbf{C})$, then the conditions of the theorem are satisfied if

$$t \leq \lfloor \frac{d_{\min}(\mathbf{C}) - 1}{2} \rfloor;$$

hence the quantity $\lfloor (d_{\min}(\mathbf{C}) - 1)/2 \rfloor$ is often referred to as the *error-correcting capability* of the code \mathbf{C} . For example, if $d_{\min}(\mathbf{C}) = 3$ or 4 , then \mathbf{C} is single error-correcting; if $d_{\min}(\mathbf{C}) = 5$ or 6 , then \mathbf{C} is double error-correcting; etc.

A classical problem in code design is as follows: given an alphabet A , a certain block length n , and a desired minimum distance d , design a code \mathbf{C} of length n over A having $d_{\min}(\mathbf{C}) \geq d$ and as many codewords as possible. This is indeed an extremely difficult problem in general.

2 Groups

So far our considerations in coding have been very general: a code of length n over an alphabet A was defined simply as a *subset* of A^n . This extreme generality is a great hindrance, as little can be said about such general sets. The descriptive complexity of general codes is very high: to specify a code C of length n and rate R requires giving a list of $n2^{nR}$ symbols over alphabet A , which clearly becomes less and less feasible as n becomes large. Without imposing some structure on codes, it is difficult to proceed much further. Thus, in this course and in practice, most codes are *linear codes*, i.e., they are vector spaces over some finite field. To get to vector spaces over finite fields, we briefly digress to pick up a few concepts from algebra.

Richard W. Hamming (1915–1998) is regarded by many as the founder of constructive coding theory. The Hamming distance, the Hamming (sphere-packing) bound and the Hamming codes are all named in his honour. (He is also known in signal processing for the Hamming window, and in number theory for the Hamming numbers).

He was born in Chicago, Illinois and died in Monterey, California. He received his bachelor's degree from the University of Chicago in 1937, a master's degree from the University of Nebraska in 1939, and a Ph.D. from the University of Illinois at Urbana-Champaign in 1942. He was a professor at the University of Louisville during World War II, but left to work on the Manhattan Project in 1945, programming one of the earliest electronic digital computers. It was in apparent frustration with the capability of these machines to detect (but not correct) errors that he invented the Hamming codes.

Between 1946 and 1976 he worked at the Bell Telephone Laboratories, where Claude E. Shannon was one of his co-workers. In 1976 he moved to the Naval Postgraduate School in Monterey, California, where he worked as an Adjunct Professor until shortly before his death in 1998.



★ **Definition:** A *binary operation* $*$ on a set X is a mapping from $X \times X$ to X .

This mapping is written $x * y$.

Examples:

1. The set $X = \{0, 1, 2, 3, \dots\}$ with $*$ being the conventional addition operation ($+$); this yields a valid binary operation since the sum of two integers is another well-defined integer.
2. The set is \mathbb{Z} and $*$ is multiplication; this yields a valid binary operation since the product of two integers is always an integer.
3. The set is the set of 2×2 matrices with real-valued entries and the operation is matrix multiplication; this yields a valid binary operation since the product of two such matrices is another such matrix. This example shows that a binary operation need not be commutative, i.e., it is *not* necessary that $x * y = y * x$.

By definition, every binary operation on X enjoys a “closure” property, i.e., the composition of two elements of X is by definition another element of X .

We now get to a fundamental concept in algebra, that of a *group*.

★ **Definition:** A *group* G is a pair $(\hat{G}, *)$, where \hat{G} is a nonempty set and $*$ is a binary operation on \hat{G} , that satisfies the following three axioms.

1. **(associativity)**
for all $a, b, c \in \hat{G}$, $a * (b * c) = (a * b) * c$;
2. **(existence of an identity)**
there exists $e \in \hat{G}$ such that, for all $a \in \hat{G}$, $a * e = e * a = a$,
(e is an *identity* element);
3. **(existence of inverses)**
for all $a \in \hat{G}$ there exists $a^{-1} \in \hat{G}$ such that $a * a^{-1} = a^{-1} * a = e$,
(a^{-1} is an *inverse* of a).

Some people write closure as a fourth axiom but it really is implied by the definition of a binary operation. In common practice, the set of elements of a group G is often itself written as G (not \hat{G}); it should be kept in mind, however, that a group is the combination of a set and a binary operation.

Instead of $a * b$, where the group operation is denoted explicitly, we will often simply write ab to mean the same thing.

The following results follow immediately from the definition.

★ **Theorem:**

1. Every group has a unique identity element.
2. The inverse any group element is unique.

Proof:

1. Suppose that G contains two identity elements e_1 and e_2 . Then, since e_1 is an identity, $e_1e_2 = e_2$. Likewise, since e_2 is an identity, $e_1e_2 = e_1$. Thus $e_1 = e_2$, i.e., there cannot be distinct identity elements in a group.
2. Suppose that G has an element a with two inverse elements b_1 and b_2 . Then $b_1ab_2 = (b_1a)b_2 = eb_2 = b_2$. On the other hand, $b_1ab_2 = b_1(ab_2) = b_1e = b_1$. Thus $b_1 = b_2$, i.e., no element can have distinct inverse elements. ■

Examples of Groups and non-Groups

1. $(\mathbb{Z}, +)$, i.e., the set of integers under addition, is a group.
2. $(\{0, 1, 2, \dots\}, +)$, i.e., the set of non-negative integers under addition, despite having a nice closure property, is *not* a group, since nonzero elements do not have an additive inverse in the set.
3. (\mathbb{Z}, \times) , i.e., the set of integers under multiplication, is *not* a group, since some elements, e.g., 2, don't have multiplicative inverses in \mathbb{Z} .
4. $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$ (the set of invertible 2×2 matrices) forms a group under matrix multiplication. In this group, it is not true that $AB = BA$ for all A and B , i.e., this is an example of a group with a non-commutative operation.
5. $(\mathbb{Z}_m, + \text{ mod } m) = (\{0, 1, \dots, m-1\}, + \text{ mod } m)$ is a group. Here the operation is addition modulo m , which works just like ordinary integer addition, except that values that fall outside the set are reduced back into the set by adding or subtracting an appropriate multiple of m .

The binary operation in a finite group can be displayed explicitly in a “multiplication table” or “group table”, a square array with rows and columns corresponding to distinct group elements, and an element in row a , column b taking the value $a*b$. The elements in this table form an interesting pattern.

★ **Theorem:** Every group table is a Latin square, i.e., every group element appears exactly once in each row and column of the table.

Proof: Suppose that there is a repeated element in the row corresponding to element a . Then there would be two distinct elements b_1 and b_2 such $ab_1 = ab_2$. Then $a^{-1}ab_1 = a^{-1}ab_2$ implies $b_1 = b_2$, in contradiction to the fact that b_1 and b_2 are distinct. Thus no row can have a repeated element, and similarly no column can have a repeated element either. ■

For example, the group tables for \mathbb{Z}_2 , \mathbb{Z}_3 and \mathbb{Z}_4 are given in Fig. 1.

| | | |
|---------|-----------|-------------|
| + 0 1 | + 0 1 2 | + 0 1 2 3 |
| 0 0 1 | 0 0 1 2 | 0 0 1 2 3 |
| 1 1 0 | 1 1 2 0 | 1 1 2 3 0 |
| | 2 2 0 1 | 2 2 3 0 1 |
| | | 3 3 0 1 2 |
| (a) | (b) | (c) |

Figure 1: Group tables for (a) \mathbb{Z}_2 , (b) \mathbb{Z}_3 and (c) \mathbb{Z}_4 .

It is sometimes the case that the group operation is commutative, in which case the group is called *abelian*¹.

* **Definition:** A group $(\hat{G}, *)$ is *abelian* if its group operation is commutative, i.e., the operation $*$ satisfies a fourth axiom:

4. (**commutativity**)
for all $a, b \in \hat{G}$, $a * b = b * a$.

Among the groups given above, \mathbb{Z} and \mathbb{Z}_m are abelian. Abelian groups are often written using “additive notation,” i.e., the operation is denoted ‘+’, the identity element is denoted 0, and the inverse of element a is denoted as $-a$.

3 Subgroups and Cosets

Let $(G, *)$ be a group with group and let H be a nonempty subset of G . In some cases it may happen that the binary operation, when restricted to H , forms a binary operation on H , i.e., for all $h_1, h_2 \in H$, we have $h_1 * h_2 \in H$. If, in addition, we have $h \in H$ implies $h^{-1} \in H$, then H is called a *subgroup* of G .

In fact, $(H, *)$ (with $*$ restricted to H) is itself a group, because it satisfies all of the axioms that define a group:

1. associativity holds in H because it holds in G , i.e., associativity is *inherited* from G ;
2. H contains the identity element, since if $h \in H$ then $h^{-1} \in H$, therefore $h * h^{-1} = e \in H$;
3. each element of H has an inverse by assumption.

Clearly G is a (trivial) subgroup of itself. Likewise, the set $H = \{e\}$, consisting of just the identity element of G forms a (trivial) subgroup of G . In \mathbb{Z}_4 , the set $H =$

¹In honor of the Norwegian mathematician Niels Henrik Abel (1802-1829), who managed to accomplish several significant tasks in mathematics despite a life tragically cut short by tuberculosis.

$\{0, 2\}$, clearly closed under $+$ and the taking of additive inverses, forms a subgroup. In the group of invertible 2×2 matrices over \mathbb{R} under matrix multiplication, the subset of matrices having unit determinant forms a subgroup.

Let H be a subgroup of G . For any $g \in G$ the set

$$gH = \{gh : h \in H\}$$

is called a *left coset* of H and similarly the set

$$Hg = \{hg : h \in H\}$$

is called a *right coset* of H . (If G is abelian, then $gH = Hg$, so the distinction between left and right cosets becomes immaterial.) In the following, though we will focus on left cosets, all of our observations will translate in an obvious way to right cosets as well.

The first observation about cosets of H is that every element of G is contained in one. Let us denote the group identity as e . Since $e \in H$ (as H is a subgroup), then $g \in gH$, as $g = ge$, and so it satisfies the defining property for membership in gH . It follows that the cosets of H in G form a cover² of G .

The next observation about the cosets of H is that two cosets either are disjoint or they coincide (i.e., if they have *any* elements in common, they have *all* of their elements in common). This is expressed by the following theorem.

★ **Theorem:** Let H be a subgroup of G . If g_1H and g_2H are two cosets of H with $g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$.

Proof: Suppose that g_1H and g_2H both contain the element c . Then $c = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. It follows that $g_1 = ch_1^{-1}$.

Now let a be an arbitrary element of g_1H . Then, for some $h_3 \in H$, we have

$$a = g_1h_3 = ch_1^{-1}h_3 = g_2h_2h_1^{-1}h_3 = g_2h_4,$$

where $h_4 = h_2h_1^{-1}h_3 \in H$. Thus $a \in g_2H$, and hence $g_1H \subseteq g_2H$. By a similar argument we may show that $g_2H \subseteq g_1H$. Thus $g_1H = g_2H$. ■

Thus, not only do the cosets of H form a partition of G , they form the nicest sort of partition: a *disjoint partition*. This observation leads to a very nice theorem known in group theory as *Lagrange's Theorem*.

★ **Theorem:** (Lagrange) Let H be a subgroup of a finite group G . Then $|H|$ is a divisor of $|G|$, i.e., $|G|/|H|$ is an integer.

Proof: Since G is finite, so must be H .

We first show that every coset of H has the same number of elements. Let $h_1, h_2, \dots, h_{|H|}$ denote the distinct elements of H . Then $gH = \{gh_1, gh_2, \dots, gh_{|H|}\}$.

²A *cover* of a set X is a collection of nonempty subsets of X whose union is X .

If, for some i and j we have $gh_i = gh_j$, we would have (upon multiplication on the left by g^{-1}) $h_i = h_j$, thus i cannot be distinct from j . It follows that $gh_1, gh_2, \dots, gh_{|H|}$ are all distinct, and so $|gH| = |H|$.

Suppose there are m distinct cosets of H in G . Since the cosets of H form a disjoint partition of G , and each coset has $|H|$ elements, it follows that $|G| = m|H|$.

■