LOOP TRANSVERSAL CODES

Jonathan D.H. Smith

Department of Mathematics
Iowa State University
Ames, IA 50011, USA

1. Introduction.

Reliable storage and transmission of information is one of the fundamental requirements of modern society. When a patient's medical data are recorded in a hospital's database, it is vitally important that a doctor prescribing medicine or performing surgery recovers the data from the database exactly as they were written in. When a bank transfers funds electronically from one account to another, the figures recording the amount being transferred must not be subject to change during the transmission. A compact disk is expected to provide perfect quality of reproduction, even when the disk is scratched or dusty. At the heart of the technology guaranteeing the reliability of information transmission through space or time lies the mathematical discipline of algebraic coding theory. Traditionally, this discipline has relied on relatively elaborate mathematical machinery such as Galois theory or algebraic geometry. This article shows how much simpler mathematical structures – loops and quasigroups – may be used to construct codes for the correction of errors in information transmission.

2. Quasigroups and loops.

A *quasigroup* Q or $(Q, \cdot)$ is a set Q equipped with a binary multiplication, denoted by $\cdot$ or juxtaposition, such that in the equation

$$x \cdot y = z, \tag{2.1}$$

knowledge of any two of x, y, z specifies the third uniquely. Thus for each element q of Q, the *right multiplication*

$$R(q) \ : \ Q \to Q; \ x \mapsto xq \tag{2.2}$$

and *left multiplication*

$$L(q) \ : \ Q \to Q; \ x \mapsto qx \tag{2.3}$$

are elements of the group $Q!$ of bijections or permutations of the set Q. A quasigroup may be redefined equivalently as a set Q with three binary operations, namely the multiplication, *right division*

$$x/y = xR(y)^{-1} \tag{2.4,}$$

and *left division*

$$x \setminus y = yL(x)^{-1}. \tag{2.5}$$

These three operations are required to satisfy the identity

$$(xy)/y = x \tag{2.6}$$

showing that $R(y)$ injects (i.e. $xR(y) = x'R(y) \implies x = xR(y)/y = x'R(y)/y = x'$), the identity

$$(x/y)y = x \tag{2.7}$$

showing that $R(y)$ surjects (i.e. $x \in Q \implies x = (x/y)R(y)$), the identity

$$y \setminus (yx) = x \tag{2.8}$$

showing that $L(y)$ injects, and the identity

$$y(y \setminus x) = x \tag{2.9}$$

showing that $L(y)$ surjects.

Example 2.1. Any group G forms a quasigroup $(G, \cdot, /, \backslash)$ with $x/y = xy^{-1}$ and $x \backslash y = x^{-1}y$. $\square$

A group is required to satisfy the associative identity

$$(xy)z = x(yz) \tag{2.10}$$

for its multiplication. In a general quasigroup, this requirement is dropped. For this reason, quasigroups are sometimes considered as "non-associative groups".

Example 2.2. The set $\mathbb{Z}$ of integers forms a quasigroup using the non-associative operation of subtraction as the "multiplication". Certainly, in the equation $x - y = z$, knowledge of any two of x, y, z specifies the third uniquely. $\square$

Example 2.3. A *Latin square* on an n-element set is an $n \times n$ square array in which each column and each row contains each element of the set exactly once. For example,

$$\begin{array}{ccc|ccc} 1 & 3 & 2 & 5 & 6 & 4 \\ 3 & 2 & 1 & 6 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 & 6 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 6 & 4 & 2 & 3 & 1 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{array} \tag{2.11}$$

is a Latin square on the set $Q = \{1, 2, 3, 4, 5, 6\}$. Given a Latin square on a set, one may make the set into a quasigroup by labelling the rows and columns of the Latin square with the elements of the set in some order, thus obtaining the multiplication table for the quasigroup. For instance, the Latin square (2.11) yields a quasigroup Q with multiplication table

$$\begin{array}{c|ccc|ccc} Q & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 3 & 2 & 5 & 6 & 4 \\ 2 & 3 & 2 & 1 & 6 & 4 & 5 \\ 3 & 2 & 1 & 3 & 4 & 5 & 6 \\ \hline 4 & 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 5 & 6 & 4 & 2 & 3 & 1 \\ 6 & 6 & 4 & 5 & 3 & 1 & 2 \end{array}. \tag{2.12}$$

Thus in Q, one has $4 \cdot 2 = 5$, etc. Conversely, note that the multiplication table of any finite quasigroup will yield a Latin square by deleting the left and upper borders. $\square$

A quasigroup Q or $(Q, \cdot, /, \backslash)$ is said to be a *loop* if it has a special element, usually denoted by 1 and known as the *identity element*, such that Q satisfies the laws

$$x \cdot 1 = x = 1 \cdot x. \tag{2.13}$$

Note that groups are loops. On the other hand, the quasigroups of Examples 2.2 and 2.3 do not contain identity elements. The multiplication table

(2.14)

Q	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

exhibits a non-associative loop of order 5.

3. Right loops and loop transversals.

In §2, a quasigroup Q was specified as a set-with-structure $(Q, \cdot, /, \backslash)$ satisfying (2.6-9). This specification breaks up naturally into left- and right-handed parts that share the multiplication. Taking the right-hand part alone, a *right quasigroup* $(Q, \cdot, /)$ is a set equipped with a binary *multiplication* $\cdot$ and *right division* $/$ such that (2.6) and (2.7) are satisfied. Recall that (2.6) yields the injectivity of each right multiplication, while (2.7) yields its surjectivity. The right division x/y is then expressed in the form $xR(y)^{-1}$ of (2.4).

Example 3.1. Let Q be a set. Define $x \cdot y = x = x/y$ for x, y in Q. Then $(Q, \cdot, /)$ is a right quasigroup, with $R(y) = 1$ for all y in Q. $\square$

Restriction from right quasigroups to right loops eliminates trivialities such as those inherent in Example 3.1. A *right loop* $(Q, \cdot, /, 1)$ is a right quasigroup $(Q, \cdot, /)$ with an *identity element* 1 satisfying (2.13). A *right quasigroup homomorphism* is defined to be a

set map $f : Q \to P; q \mapsto q^f$ between right quasigroups $(Q, \cdot, /)$ and $(P, \cdot, /)$ that preserves the multiplication and right division. In other words, $x^f \cdot y^f = (x \cdot y)^f$ and $x^f / y^f = (x/y)^f$ for all x, y in Q. (Note the algebraic convention of writing functions to the right of their arguments, as with the squaring function $x \mapsto x^2$. This convention makes it much easier to read the action of composite functions, and helps to reduce the number of brackets required.) A *right loop homomorphism* is a right quasigroup homomorphism between right loops mapping the identity of the domain to the identity of the codomain. A *right loop isomorphism* is just a bijective right loop homomorphism. Of course, one may also study oppositely-handed versions of the above, namely left quasigroups, left loops, etc.

The primary sources of right loops are right transversals to subgroups of groups. Let H be a subgroup of a group $(G, \cdot, /, \backslash, 1)$, and let T be a right transversal to H in G such that 1 represents H. (Transversals having the identity as the representative for the subgroup are often described as *normalized*.) Thus the group G is partitioned as $G = \bigcup_{t \in T} Ht$ into a disjoint union of cosets Ht of H, indexed by the elements t of the transversal T. Define a map $\varepsilon : G \to T; g \mapsto g^\varepsilon$ by

$$g \in Hg^\varepsilon, \tag{3.1}$$

so that g^ε or $g\varepsilon$ is the unique representative in T for the right coset of H that contains g. It is also convenient to define a map $\delta : G \to H; g \mapsto g^\delta$ by

$$g = g^\delta g^\varepsilon. \tag{3.2}$$

Note that $1^\delta = 1^\varepsilon = 1$. Moreover $h^\delta = h$ and $h^\varepsilon = 1$ for h in H, while $t^\delta = 1$ and $t^\varepsilon = t$ for t in T. Now define a binary multiplication $*$ and a binary right division $\|$ on T by

$$t * u = (tu)\varepsilon,\ t \| u = (t/u)\varepsilon \tag{3.3}$$

for t, u in T, i.e. by $tu \in H(t * u)$ and $t/u = tu^{-1} \in H(t \| u)$. Since $H(t \| u)u \ni (t/u).u = t \in Ht$ and $H(t * u)/u \ni (tu)/u = t \in Ht$, one has $(t \| u) * u = t$ and $(t * u) \| u = t$ for all t, u in T. Moreover $1 * t = (1t)\varepsilon = t\varepsilon = t = t\varepsilon = (t1)\varepsilon = t * 1$. Summarizing,

Proposition 3.2. *Let T be a normalized right transversal from a group G to a subgroup H. Then $(T, *, \|, 1)$ is a right loop.* $\square$

To within right loop isomorphism, every right loop may be obtained by the construction of Proposition 3.2. Note also that the set bijection $T \to H \setminus G$; $t \mapsto Ht$ may be used to transfer the right loop structure from the normalized right transversal T to the set $H \setminus G$ of cosets of H.

In certain circumstances, the right loop of Proposition 3.2 will become a loop. If this happens, the normalized right transversal T is called a *loop transversal*. Thus T is a loop transversal if and only if, for each ordered pair (t, u) of elements of T, the equation

$$t * x = u \tag{3.4}$$

has a unique solution. The solution x is the result of t dividing u from the left in the loop.

Example 3.3. Let N be a normal subgroup of the group G. Then a normalized right transversal T from G to N is a loop transversal. Indeed, the set bijection $T \to N\backslash G; t \mapsto Nt$ becomes a right loop isomorphism $(T, *, \|, 1) \to (N \setminus G, \cdot, /, N) = (G/N, \cdot, /, N)$, since $N(t * u) = Ntu = NNtu = Nt \cdot t^{-1}Ntu = Nt \cdot Nu$. $\square$

Proposition 3.4. *Let T be a normalized right transversal from a group G to a subgroup H. Then T is a loop transversal if and only if it is a right transversal to each conjugate H^g of H in G.*

Proof. Suppose first that T is a loop transversal. Note $H^g = g^{-1}Hg = (g^\delta g^\varepsilon)^{-1}Hg^\delta g^\varepsilon = H^{g^\varepsilon}$. Then for x in T and a in G, one has $a \in H^g x \Leftrightarrow a \in H^{g^\varepsilon} x \Leftrightarrow g^\varepsilon \cdot a \in Hg^\varepsilon \cdot x \Leftrightarrow (g^\varepsilon \cdot a)\varepsilon = (g^\varepsilon \cdot x)\varepsilon \Leftrightarrow g^\varepsilon * x = (g^\varepsilon \cdot a)\varepsilon$. Since $(T, *)$ is a loop, there is a unique solution x to the latter equation. Thus T is a right transversal to H^g in G.

Conversely, suppose that T is a right transversal to each conjugate of H in G. It must be shown that (3.4) has a unique solution x. But $t * x = u \Leftrightarrow (tx)\varepsilon = u \Leftrightarrow Hu = H(tx)^\varepsilon = Htx \Leftrightarrow u \in Htx \Leftrightarrow t^{-1}u \in H^t x$. Since T is a right transversal to H^t, there is a unique x in T for which $t^{-1}u \in H^t x$, and thus for which $t * x = u$. $\square$

4. Loop transversal codes.

The concept of a loop transversal offers a quick and elementary introduction to the subject of algebraic coding theory. Algebraic coding theory addresses certain aspects of the problem of transmitting information through channels that are subject to interference. The effect of the interference is to corrupt the signals being transmitted. Nevertheless, algebraic coding theory offers methods of encoding the original information into a signal for transmission, in such a way that the original information may be recovered from a corrupt received signal, or at least so that a signal may be recognized as being corrupt. The information transmission may be taking place through space, sending a message from one physical location to another. On the other hand, it may also be taking place through time, recording a message in a memory, and then reading it back later.

The usual scheme of algebraic coding theory may be summarized as follows. A finite set A is given, known as the *alphabet*. The elements of the alphabet A are often described as the *letters* of the alphabet A. Typically, one uses the *binary alphabet* $\{0, 1\}$ consisting of the two binary digits $0, 1$ or integers modulo 2. The information to be transmitted is assembled from words of fixed length k, i.e. concatenations of k (not necessarily distinct) letters of the alphabet. This set of words to be encoded is described as the *uniform code* A^k. The information channel carries words from the uniform code A^n, for some $n \geq k$. The integer n is known as the *length* of the channel. A subset C of A^n is chosen. This subset C is known as the *code* (or a *block code* to avoid confusion with the concept of a uniform code). The *encoding* is an embedding $A^k \to A^n$ with image C, restricting to a bijection $\eta : A^k \to C$. Thus $|C| = |A|^k$. The integer k is known as the *dimension* of the code. If a word c from the code C is transmitted through the channel without corruption, then it is received as the same word c. The original encoded word from A^k may then be recovered as $c\eta^{-1}$. However, the emitted codeword c may have been subject to interference in the channel, being received as a corrupted word x in A^n. A *decoding* map

$$\delta : A^n \to C \tag{4.1}$$

assigns a codeword x^δ to the received word x. Provided that the received word x was not

corrupted excessively from the emitted codeword c, one should expect that $x^\delta = c$. In particular, one should have $c^\delta = c$ for c in C.

Example 4.1(Repetition codes). Let $A = \{0, 1\}$ and $k = 1$. Consider a channel length of 3. Define $0\eta = 000$ and $1\eta = 111$. Thus $C = \{000, 111\}$. Define the decoding (4.1) by $\delta^{-1}\{000\} = \{000, 001, 010, 100\}$ and $\delta^{-1}\{111\} = \{111, 110, 101, 011\}$ ("majority vote"). Provided that at most one letter of the emitted codeword gets corrupted in the channel, the decoder is able to recover the codeword. One may extend this scheme to channels of greater odd length. □

For further analysis, it is convenient to put an abelian group structure $(A, +, 0)$ on the alphabet A. Usually, for $|A| = l$, one takes A to be the cyclic group $(\mathbb{Z}_l, +, 0)$ of residues modulo l. The channel A^n is the n-th direct power of A, with componentwise operations. Thus the channel A^n becomes the abelian group $(A^n, +, 0)$, or more pedantically $(A^n, +, 00\dots0)$. This abelian group structure may be used to describe the interference taking place in the channel. If an emitted codeword c is received as the corrupted word x, one says that the *error* $x - c$ was added to c during passage through the channel. The decoder $\delta : x \mapsto c$ is then said to *correct* the error $x - c$. To measure the seriousness of the error, one may define the *Hamming weight* $|x|$ of a channel word x in A^n to be the number of non-zero letters in x. The *Hamming distance* between two words x, y is then $|x - y|$. Note that the triangle inequality

$$|x + y| \leq |x| + |y| \tag{4.2}$$

is satisfied. Indeed, $|x + y| > |x| + |y|$ is impossible, since $x + y$ can only have a non-zero letter in a certain slot if at least one of x and y has a non-zero letter in that slot. Moreover, $|x| = 0 \Leftrightarrow x = 0$.

The decoding may be analyzed using the abelian group structure. An *error map*

$$\varepsilon : A^n \to A^n \tag{4.3}$$

determines that a received word x was the result of an error x^ε. Thus

$$x = x^\delta + x^\varepsilon \tag{4.4}$$

for each x in A^n. The key idea behind loop transversal codes is the observation that (4.4) may just be an instance of (3.2). Thus the code C is defined to be *linear* if it is a subgroup of the channel A^n. Since A^n is abelian, such a subgroup C is normal. As in Example 3.3, any normalized right transversal T to C in A^n is then a loop transversal. Taking the error map ε as in (3.1), one obtains the loop transversal T as the set of errors corrected by the code. Note that the loop $(T, *, 0)$ defined by (3.3) is an abelian group, since the map $T \to A^n/C; t \mapsto C + t$ of Example 3.3 is a right loop isomorphism of T with the abelian group A^n/C. Nevertheless, it is often convenient to continue to refer to the operation $*$ as a loop multiplication, in order to distinguish it from the abelian group operation $+$ on A^n.

Example 4.2. Consider the length 3 binary repetition code C of Example 4.1. Interpret A as $\mathbb{Z}_2$. Then C becomes linear, and the normalized right transversal $T = \{000, 001, 010, 100\}$ is the set of errors corrected by C. The abelian group multiplication $*$ on T given by (3.3) has the table

$*$	000	001	010	100
000	000	001	010	100
001	001	000	100	010
010	010	100	000	001
100	100	010	001	000

.

Note that the table may be summarized by the specification that the map

$$s : (T, *) \to (A^2, +); 001 \mapsto 01, 010 \mapsto 10, 100 \mapsto 11$$

is an abelian group homomorphism. □

If one knows a linear code C in a channel A^n, one may determine a loop transversal T to C by selecting representatives of the various cosets of C. Typically, one picks *coset leaders*–representatives having minimal Hamming weight within their cosets. On the other hand, one of the major problems of algebraic coding theory is to determine a suitable code C to begin with, for a given channel A^n. If the loop $(T, *, 0)$ is known, then the code C may be obtained from T by the so-called *Principle of Local Duality*. To formulate

this principle, it is convenient to establish some notation. For elements $t_1, t_2, \ldots$ of T, define $\sum_{i=1}^{m} t_i$ inductively by $\sum_{i=1}^{0} t_i = 0$ and $\sum_{i=1}^{m} t_i = t_m + \sum_{i=1}^{m-1} t_i$. Define $\prod_{i=1}^{m} t_i$ inductively by $\prod_{i=1}^{0} t_i = 0$ and $\prod_{i=1}^{m} t_i = t_m * \prod_{i=1}^{m-1} t_i$. In compound expressions involving loop operations $*, \|$ and abelian group operations $+, -$, the loop operations will bind more strongly than the group operations. For example, $t + u - t * u = t + u - (t * u)$.

Proposition 4.3 (Principle of Local Duality). *Let T be a loop transversal to a linear code C in a channel A^n, over a finite abelian group alphabet A. Suppose that T is a set of generators for A^n. Then $C = \{\sum_{i=1}^{m} t_i - \prod_{i=1}^{m} t_i \big| \langle t_1, \ldots, t_m \rangle \in T^{*\kappa}\}$.*

Proof. Recall that $t^{\varepsilon} = t$ for t in T. Induction on m using (3.3) then shows that $\left(\sum_{i=1}^{m} t_i\right)\varepsilon = \prod_{i=1}^{m} t_i$ for $t_1, \ldots, t_m$ in T. Since T generates A^n and A is finite, each channel word x may be written in the form $x = \sum_{i=1}^{m} t_i$ for some multisubset $\langle t_1, \ldots, t_m \rangle$ of T. Then $C = \{x^{\delta} | x \in A^n\} = \{x - x^{\varepsilon} | x \in A^n\} = \left\{ \sum_{i=1}^{m} t_i - \prod_{i=1}^{m} t_i \middle| \langle t_1, \ldots, t_m \rangle \in T^{*\kappa} \right\}$. $\square$

The full force of the Principle of Local Duality comes into play when it is not even known in advance that there is some code C to which a loop $(T, *, 0)$ in A^n is transversal. For simplicity, the case $A = \mathbb{Z}_2 = \{0, 1\}$ will be discussed here. Given a channel A^n, one normally has a list of the errors one would like to correct (e.g. the commonest errors), and this list usually includes the n-element set B of errors of Hamming weight 1. Let T be a 2^{n-k}-element set of errors to be corrected, with $T \supseteq \{0\} \cup B$. Suppose that T carries a loop structure $(T, *, 0)$ given by an isomorphism

$$s : (T, *, 0) \to (A^{n-k}, +, 0) \tag{4.5}$$

(e.g. as in Example 4.2). Let $t_1, \ldots, t_m$ be elements of T. By the closure of $(T, *)$, the loop product $\prod_{i=1}^{m} t_i$ always lies in T. On the other hand, the sum $\sum_{i=1}^{m} t_i$ may only lie in T for certain choices of $t_1, \ldots, t_m$. The isomorphism (4.5) is said to be a *partial homomorphism* $s : (T, +) \to (A^{n-k}, +)$ if $\left(\sum_{i=1}^{m} t_i\right) s = \sum_{i=1}^{m} t_i^s$ whenever $\sum_{i=1}^{m} t_i \in T$. Of course, this means that $\sum_{i=1}^{m} t_i = \prod_{i=1}^{m} t_i$ in such cases, since the two sides of the equation have the same image under the isomorphism (4.5).

Theorem 4.4. *Let T be a 2^{n-k}-element subset of the length n binary channel A^n, such that T contains 0 and the n-element set B of errors of Hamming weight 1. Suppose that T carries a loop structure $(T, *, 0)$ given by an isomorphism (4.5) such that $s : (T, +) \to (A^{n-k}, +)$ is a partial homomorphism. Then there is a linear code C of dimension k in A^n to which $(T, *, 0)$ is a loop transversal. Moreover, T is precisely the set of errors corrected by C.*

Proof. Note that each element x of A^n has a unique expression $x = \sum\{b_i | i \in X\}$ for a subset X of B. Define the *syndrome*

$$s : A^n \to A^{n-k}; \sum_{i\in X} b_i \mapsto \sum_{i\in X} b_i^s. \tag{4.6}$$

Since (4.5) is a partial homomorphism, it is the restriction of the syndrome to T. Now for x, y in A^n, with $x = \sum\limits_{i\in X} b_i$ and $y = \sum\limits_{i\in Y} b_i$, one has

$$x^s + y^s = \sum_{i\in X} b_i^s + \sum_{i\in Y} b_i^s = \sum\{b_i^s | i \in (X \cup Y) - (X \cap Y)\} = (x + y)s.$$

Thus the syndrome is an abelian group homomorphism. Let $C = \mathrm{Ker}\ s$ be its group kernel $s^{-1}\{0\}$. Note that $|C| = |A|^k$. For $x = \sum\limits_{i\in X} b_i$ in A, define $x^\delta = \sum\limits_{i\in X} b_i - \prod\limits_{i\in X} b_i$ and $x^\varepsilon = \prod\limits_{i\in X} b_i$. Then $x^\delta \in C$ and $x^\varepsilon \in T$, with $x = x^\delta + x^\varepsilon$. Thus $A^n = C + T$. But $|A^n| = |C|.|T|$, so T is a loop transversal to C in A^n. Moreover, $\delta : A^n \to C; x \mapsto x^\delta$ and $\varepsilon : A^n \to T; x \mapsto x^\varepsilon$ surject, indeed $\varepsilon|_T = 1_T$, so T is precisely the set of errors corrected by C. □

5. A code for hexadecimal digits.

For the alphabet $\mathbb{Z}_2 = \{0, 1\}$, consider the set $\mathbb{Z}_2^4 = \{0 = 0000, 1 = 0001, 2 = 0010, \ldots, 9 = 1001, A = 1010, B = 1011, \ldots, F = 1111\}$ of hexadecimal digits. This set is to be encoded for transmission through a binary channel of length 7 in such a way that errors of single Hamming weight may be corrected. Let b_i, for $1 \le i \le 7$, denote the binary word of length 7 and Hamming weight 1 with its unique non-zero letter in the i-th slot. Thus $b_1 = 1000000, \ldots, b_3 = 0010000$, etc. Set $B = \{b_i | 1 \le i \le 7\}$ and

$T = \{0000000\} \cup B$. Define $s : T \to \mathbb{Z}_2^3 = \mathbb{Z}_2^{7-4}$ as a partial homomorphism by sending b_i to the binary representation of i, e.g. $b_3^s = 011$. This sets up an isomorphism (4.5), e.g. $b_1 * b_3 = (b_1^s + b_3^s)s^{-1} = (001 + 011)s^{-1} = 010s^{-1} = b_2$. By Theorem 4.4, the loop transversal $(T, *, 1)$ then determines a code C of dimension 4. The 2^4 hexadecimal digits may be encoded by bijection with C. The elements of C may be determined by the Principle of Local Duality, e.g. $b_1 + b_3 - b_1 * b_3 = 1000000 + 0010000 - 0100000 = 1110000 \in C$.

Exercise.

(a) Using the Principle of Local Duality, and the fact that the code is a subgroup of the channel, determine all 16 codewords. [Hint: along with 0000000, there should be seven codewords of Hamming weight 3, seven codewords of Hamming weight 4, and one codeword of Hamming weight 7.]

(b) Set up an encoding bijection $\eta : \mathbb{Z}_2^4 \to C$. [Hint: there is considerable choice here.]

(c) If the hexadecimal digit E is encoded, and subjected to the error b_4 during passage through the channel $\mathbb{Z}_2^7$, show that it may be recovered.

(d) If the hexadecimal digit E is encoded, and subjected to the error $b_2 + b_4$, to which hexadecimal digit is the received word decoded? [Hint: the answer depends on your choice of η in (b).]

6. Further reading.

For an elementary introduction to quasigroups and loops, one may consult [1, 6, 8]. More advanced topics are covered in [3]. The fundamentals of the traditional approach to coding theory are presented in [2, 9], while [10] describes the application of algebraic geometry to coding theory. The loop transversal approach discussed here was initiated in [7], and further theoretical aspects are treated in [5]. In [4], the loop transversal method is applied to produce record-breaking binary and ternary codes using a simple "greedy" algorithm to construct the isomorphism (4.5).

References.

[1] A. Almeida Costa, *Cours d'Algèbre Générale*, Fundação Calouste Gulbenkian, Lisboa, 1969.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, NY, 1968.

[3] O. Chein, H. Pflugfelder and J.D.H. Smith (eds.), *Quasigroups and Loops : Theory and Applications*, Heldermann, Berlin, 1990.

[4] F.-L. Hsu, F.A. Hummer and J.D.H. Smith, *Logarithms, syndrome functions, and the information rate of greedy loop transversal codes*, J. of Comb. Math. and Comb. Comp. **22** (1996), 33–49.

[5] F.A. Hummer and J.D.H. Smith, *Greedy loop transversal codes, metrics, and lexicodes*, J. of Comb. Math. and Comb. Comp. **22** (1996), 143–155.

[6] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[7] J.D.H. Smith, *Loop transversals to linear codes*, J. of Comb., Info. and System Sci. **17** (1992), 1–8.

[8] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[9] J.H. van Lint, *Introduction to Coding Theory*, Springer, New York, NY, 1982.

[10] J.H. van Lint, *Algebraic geometric codes*, in "Coding Theory and Design Theory Part I: Coding Theory", (ed. D. Ray-Chaudhuri), Springer, New York, NY, 1990, 137–162.