UNIQUE FACTORIZATION IN CAYLEY ARITHMETICS AND CRYPTOLOGY

by P. J. C. LAMONT

(Received 26 February, 1990)

1. Introduction. Let $\mathscr{C}$ be the classical Cayley algebra defined over the reals with basis $\{i_s\}_0^7$ where $\{i_s\}_0^3$ gives a quaternion algebra $\mathscr{H}_4$ with $i_0 = 1$, $i_1 i_2 i_3 = -1$, $i_1 i_4 = i_5$, $i_2 i_4 = i_6$ and $i_3 i_4 = i_7$. The multiplication table of the imaginary basic units follows:

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	$-i_0$	i_3	$-i_2$	i_5	$-i_4$	$-i_7$	i_6
i_2	$-i_3$	$-i_0$	i_1	i_6	i_7	$-i_4$	$-i_5$
i_3	i_2	$-i_1$	$-i_0$	i_7	$-i_6$	i_5	$-i_4$
i_4	$-i_5$	$-i_6$	$-i_7$	$-i_0$	i_1	i_2	i_3
i_5	i_4	$-i_7$	i_6	$-i_1$	$-i_0$	$-i_3$	i_2
i_6	i_7	i_4	$-i_5$	$-i_2$	i_3	$-i_0$	$-i_1$
i_7	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	$-i_0$.

For $\xi = \sum_{s=0}^{7} x_s i_s$, $\bar{\xi} = 2x_0 - \xi$ is called the conjugate of ξ. The real part $\mathrm{R}(\xi)$ of the octant ξ is x_0. For $\xi = \xi_0 + \xi_1 i_4$ and $\eta = \eta_0 + \eta_1 i_4$ where ξ_t and η_t belong to $\mathscr{H}_4$ for $t = 0$ and 1, multiplication is given in $\mathscr{C}$ by

$$\xi\eta = \xi_0\eta_0 - \bar{\eta}_1\xi_1 + (\eta_1\xi_0 + \xi_1\bar{\eta}_0)i_4. \tag{1.1}$$

The norm $N\xi$ of ξ is $\xi\bar{\xi}$. Hence for any ξ of $\mathscr{C}$

$$\xi^2 - 2\mathrm{R}(\xi)\xi + N\xi = 0. \tag{1.2}$$

The multiplicative property

$$N(\alpha\beta) = N(\alpha)N(\beta) \tag{1.3}$$

holds for all octants α and β in $\mathscr{C}$.

Let J be any arithmetic or order of $\mathscr{C}$. Let a code f be defined using a subset of elements, of possibly fixed norm, of a possibly fixed J as codewords. Then f is a mapping from an alphabet

$$A = \{w_1, \ldots, w_m\}$$

into Σ^* where Σ^* denotes the collection of finite strings of symbols from an alphabet Σ. Here Σ can be regarded as the union of the integers $\mathbb{Z}$ and the half odd integers. The elements $f(w_s)$ are in J. Examples are to be found in Section 5.

A frame is a set of codewords that is encrypted together as a single octant and decrypted without causing difficulty on the available machinery. An important aspect of the codes in data transmission may be that frames of codewords admit encryption using Cayley multiplication and decryption using the algorithm to be explained. The codewords

$f(w_s)$ and their characteristic units may be varied according to their position in a frame. The unique factorization properties of Cayley arithmetics J are of importance for the algorithm and theory.

2. The maximal arithmetics J_a. An arithmetic (order) J of $\mathscr{C}$ is a subset which contains 1, is closed under addition and multiplication, and is such that for any $\xi \in J$, (1.2) has rational integral coefficients (has coefficients belonging to a ring of integers of an algebraic number field or other field). An arithmetic (order) J_a is called maximal if it is not a proper subset of an arithmetic (order defined over the same field).

Let J_0 be the arithmetic spanned by $\{i_s\}_0^7$ over $\mathbb{Z}$. Let a, u, v, w be distinct elements of $\{i_s\}_1^7$ such that $a = u(vw)$. The mapping $\xi \to \rho\xi\rho^{-1}$ where

$$\rho = \tfrac{1}{2}(1 + u + v + w)$$

applied to $\{i_s\}_0^7$ gives a new basis $\{e_s\}_0^7$ of $\mathscr{C}$ that reproduces the multiplication table of the first basis. Let J_a be the arithmetic obtained by adjoining $\{e_s\}_0^7$ to J_0. J_a is independent of the choice of u, v, w for which $u(vw) = a$ and is one of seven isomorphic maximal arithmetics. Arithmetics are obtained by letting a take any value from the set $\{i_s\}_1^7$. Intersections, consisting of all elements common to two or more orders, also yield useful orders.

Each J_a contains fourteen distinct sets of elements of the form $\sum_{r=1}^{4} x_r v_r$ where the x_r are half odd integers. The v_r take fourteen sets of values from $\{i_s\}_0^7$.

Suppose that, for some J,

$$\xi \equiv \xi_1 \pmod{2 \text{ in } J}$$

and that $\xi_1 = \Sigma x_s \rho_s$ where the ρ_s are spanning units of J. Define the characteristic unit of ξ to be

$$\chi(\xi) = \|\Pi \rho_s\|$$

where $|\pm\alpha|$ is always α for α a member of the spanning units with leading coefficient positive.

THEOREM 2.1. *For $\xi, \eta \in J_0$,*

$$\chi(\xi + \eta) = |\chi(\xi)\chi(\eta)|$$

and for ξ, η both of odd norm,

$$\chi(\xi\eta) = |\chi(\xi)\chi(\eta)|.$$

Proof. The proof is by linearization from the corresponding results for the spanning units.

3. Divisibility. Let ζ and ξ be elements of order J of $\mathscr{C}$.

THEOREM 3.1. *Suppose that $\zeta \equiv \xi \pmod{m}$ where $N\xi = m$. Then ξ divides ζ on the left and on the right.*

Proof. Since $\zeta = \xi + m\sigma$ for some $\sigma \in J$, we have $\zeta = \xi(1 + \bar{\xi}\sigma)$ by the alternative law in $\mathscr{C}$. The proof of right divisibility is similar.

https://doi.org/10.1017/S0017089500008326 Published online by Cambridge University Press

THEOREM 3.2. *Suppose that* $\zeta \equiv \xi\sigma \pmod{m}$ *where* $N\xi = m$ *and* $\sigma \in J$. *Then* ξ *divides* ζ *on the left.*

Proof. $\zeta = \xi\sigma + m\rho = \xi(\sigma + \bar{\xi}\rho)$.

Similarly we can prove the following result.

THEOREM 3.3. *Suppose that*

$$\zeta \equiv \sigma\xi \pmod{m} \quad \text{where} \quad N\xi = m \quad \text{and} \quad \sigma \in J.$$

Then ξ *divides* ζ *on the right.*

Next we have

THEOREM 3.4. *For any* $\xi \in J_a$ *of odd norm,*

$$\xi \equiv \tau \pmod{2 \text{ in } J_a}$$

where τ *is, apart from sign, a unique unit of* J_a.

Proof. The existence of fourteen distinct sets of elements of the form $\sum_{r=1}^{4} x_r v_r$ where the x_r are half odd integers ensures that the theorem holds.

We state the following results on arithmetics proved in Lamont [**8**]. Theorem 3.4 and results similar to results in Rankin [**13**] are used to satisfy the axioms in [**8**] for J_a.

THEOREM 3.5. *Any element* $\zeta \in J$ *with* $N\zeta = mn$ *has precisely* r *different factorizations* $\xi\eta$ *in* J *with* $N\xi = m$ *and* $N\eta = n$, *if* $(m, n) = 1$ *and* r *is the number of distinct units in* J. *Moreover, for* m *odd, the factorization is unique apart from signs if a unit is prescribed to which* ξ *is congruent modulo* 2 *in some* J_a.

For $\zeta \in J$ and $N\zeta = mn$, $s_J(\zeta, m, n)$ denotes the number of distinct factorizations $\delta\gamma$ of ζ in J with $N\delta = m$ and $N\gamma = n$. When no confusion can arise we omit the subscript J.

THEOREM 3.6. *For* σ *any unit in* J,

$$s(\zeta, m, n) = s(\zeta\sigma, m, n).$$

We define $r_J(m)$ to be the number of distinct elements of norm m in J. Any element $\zeta \in J$ of odd norm is called *primitive* in J if $\zeta \not\equiv 0 \pmod{p}$ for any rational prime p.

THEOREM 3.7. *Any element* $\zeta \in J$, *with* $N\zeta = p^{t+1}$, *where* p *is an odd rational prime and* t *is a positive integer, has precisely*

(i) $r(p)$ *distinct factorizations* $\xi\eta$ *with* $N\xi = p$ *and* $N\eta = p^t$, *if* $\zeta \equiv 0 \pmod{p}$;

(ii) r *such factorizations, if* ζ *is primitive in* J. *Moreover, for* ζ *primitive, unique factorization holds in the sense explained in Theorem* 3.5.

4. Unique factorization algorithm. Let a Cayley integer $\alpha \in J_a$ be given of composite (i.e. not prime and not unit) odd norm. Suppose that we are always going to divide out on the left to obtain a factorization. For example, for five factors, the parentheses pattern is assumed to be

$$\eta\{\xi[\zeta(\gamma\delta)]\}.$$

https://doi.org/10.1017/S0017089500008326 Published online by Cambridge University Press

Suppose that

$$N\alpha = \prod_{i=1}^{s} m_i$$

where the m_i, the norms of codewords, are all equal or, for example purposes, relatively prime in pairs. If the m_i are equal, α is assumed to be primitive. If the m_i are relatively prime in pairs, they are assumed ordered. Suppose that the ordered residues modulo 2 in J_a of the factors are $k_1, k_2, \ldots, k_s$.

The steps of the algorithm are as follows.

(i) Calculate and factorize $N\alpha$ into rational integers so that the factors conform to the norms of codewords.

(ii) Reduce α moduli m_i for each $i = 1, \ldots, s$.

Reductions may be carried out in an arithmetic that contains all of the codewords and that gives a decrease in the norm. As the arithmetics are partially ordered, start with an arithmetic contained in J_a with the least number of units.

Suppose that

$$\alpha \equiv \alpha_i \text{ (modulo } m_i). \tag{4.1}$$

Let $N\alpha_i = n_i m_i$. If $n_i = 1$, then α_i divides α, by Theorem 3.1. Suppose $\alpha = \alpha_i\beta$. If further $\chi(\alpha_i) = k_1$, then α_i is the required factor and we can branch to (ii) with α replaced by $(1/m_i)\bar{\alpha}_i\alpha$.

(iii) Suppose that $n_i > 1$. By recomputing the congruence (4.1), since m_i is odd, we can ensure that n_i is odd. Suppose that

$$\alpha_i \equiv \beta_i \text{ (modulo } n_i). \tag{4.2}$$

Let $N\beta_i = r_i n_i$. If $r_i = 1$, then β_i divides α_i. Hence, from (4.1) and Theorem 3.2, we can find a γ_i of norm m_i that divides α on the left. If $\chi(\gamma_i) = k_i$, then γ_i is the required factor and we can branch to step (ii) with α replaced by $(1/m_i)\bar{\gamma}_i\alpha$.

(iv) If $r_i > 1$, we continue with reduction modulo r_i in a suitable J. We can ensure that r_i is odd by modifying the congruence (4.2) if required. The process of taking moduli will necessarily terminate.

(v) At each final reduction by moduli we ensure that the residue modulo 2 in J_a of the corresponding divisor of α will be correct by multiplying by a suitable characteristic unit when advisable.

5. Examples. (i) Suppose that the word KEY is encrypted by the Cayley integers

$$\begin{aligned} \text{K:} &\quad 1 + i_2 + i_3 \\ \text{E:} &\quad 2 + i_2 \\ \text{Y:} &\quad 2i_4 + i_5 + i_6 + i_7. \end{aligned}$$

Then $\chi(\text{K}) = i_1$, $\chi(\text{E}) = i_2$, $\chi(\text{Y}) = i_4$, and $\alpha = \text{K}\{\text{EY}\} = -4i_4 + 2i_5 + 6i_6 + 7i_7$ of characteristic unit i_7.

Transmitted characteristic units or residues of codewords modulo 2 in a maximal arithmetic are called *control characters*. Here the choice of maximal arithmetic is known to the writer of the code. The list of codewords, the alphabet and, if they are used, the control characters in order are perhaps best hidden in the implementation (i.e. transparent to the user).

https://doi.org/10.1017/S0017089500008326 Published online by Cambridge University Press

Assume that α, control characters, parentheses patterns, and the fact that all codewords have all components nonnegative are known to a cryptanalyst. Here he knows that the decryption consists of three letters with control characters i_1, i_2 and i_4 in that order and can deduce the norms of codewords. He also knows that only characteristic units were used as control characters. A cryptanalyst can try to break (i.e. decrypt) the code by finding factorizations of the norm 105 octant. Suppose that we are in the position of a cryptanalyst who also knows that the word KEY is being transmitted and who decides to apply the unique factorization algorithm. To break the code, one must show that α does not factorize with first element of norm 5 nor 7 as a member of the code, but does factorize with first element of norm 3 as a member of the code.

Clearly,

$$\alpha \equiv -i_4 - i_5 + i_7 \,(\text{mod } 3 \text{ in } J_0).$$

The right-hand side of the congruence has norm 3 and characteristic unit i_6. Characteristic unit i_1 is required. Therefore, multiply by i_7 on the right to obtain $-1 - i_2 - i_3$. Hence

$$\alpha = K(3i_4 + i_5 + 4i_6 + 3i_7).$$

Reducing α mod 5 and then mod 3 we obtain in turn

$$\xi = i_4 - 3i_5 + i_6 + 2i_7, \qquad \rho = i_4 + i_6 - i_7, \qquad \chi(\rho) = i_5.$$

Characteristic unit i_1 is wanted. Therefore, multiply ρ by i_3 on the right to obtain $\rho_1 = i_4 + i_5 + i_7$. Hence $\xi = (i_1 - 2i_2)\bar{\rho}_1$. Although the factor $i_1 - 2i_2$ of norm 5 has characteristic unit i_1 and, by Theorem 3.2, must divide α on the left, it is not a codeword since it contains a negative coefficient. Now reduce α mod 7 and mod 5 in turn to obtain

$$\xi = 3i_4 - 5i_5 - i_6, \qquad \rho = 2i_4 + i_6.$$

Then

$$\xi\rho = 5(-1 + 2i_1 + i_2 + i_3).$$

Hence

$$\alpha = (1 - 2i_1 - i_2 - i_3)(3i_4 + i_5 - 2i_6 + i_7).$$

Again the element of norm 7 and of characteristic unit i_1 is not an element of the code since it contains some negative components.

Now

$$\beta = 3i_4 + i_5 + 4i_6 + 3i_7$$

represents EY. To apply the algorithm, reduce β mod 5 to obtain

$$\xi = 3i_4 + i_5 - i_6 - 2i_7.$$

ξ is of norm 15 and characteristic unit i_7. Reduce mod 3 to obtain $i_5 - i_6 + i_7$ of characteristic unit i_4. Characteristic unit i_2 is needed in the second position of the factorization of α. Multiply by i_1 on the left to obtain

$$\rho_1 = -i_4 + i_6 + i_7.$$

Then

$$\xi\rho_1 = 3(2 + i_2).$$

Thus $2 + i_2$ represents E. This completes our outline of the Example (i).

https://doi.org/10.1017/S0017089500008326 Published online by Cambridge University Press

(ii) Here we give an example of a code defined using fixed norm Cayley integers. Suppose that the word KEY is encrypted by Cayley integers as follows

$$\begin{aligned} \text{K:} &\quad 1 + i_1 + i_2 \\ \text{E:} &\quad 1 + i_1 + i_3 \\ \text{Y:} &\quad 1 + i_1 + i_4. \end{aligned}$$

Then $\chi(\text{K}) = i_3$, $\chi(\text{E}) = i_2$, and $\chi(\text{Y}) = i_5$, and

$$\alpha = \text{K}\{\text{EY}\} = -3 + 3i_1 + i_5 + 2i_6 + 2i_7$$

of characteristic unit i_4. We again adopt the role of cryptanalyst with assumptions as before. Clearly,

$$\alpha \equiv i_5 - i_6 - i_7 \,(\text{mod } 3 \text{ in } J_0).$$

Characteristic unit i_3 is needed. Multiply by i_7 on the right to obtain $\xi = 1 + i_1 + i_2$. Now

$$\alpha = (1 + i_1 + i_2)(2i_1 + i_2 + i_3 + i_4 + i_5 + i_7) = \text{K}\beta$$

where

$$\beta = i_3 + i_5 + \tfrac{1}{2}(i_1 - i_2 - i_4 - i_7) = \beta_1$$

modulo 3 in J_{i_3}, J_{i_5} or J_{i_6}. Now

$$\chi(\beta_1) = \|i_6 * \tfrac{1}{2}(i_1 - i_2 - i_4 - i_7)\|.$$

Characteristic unit i_2 is required. Multiply $\chi(\beta_1)$ on the right by i_2 to obtain, apart from sign,

$$\gamma = \tfrac{1}{2}(1 - i_3 - i_5 - i_6).$$

Now, $\beta_1\gamma = 1 + i_1 + i_3 = \text{E}$ completes the example.

6. Conclusions. Care should be exercised with arithmetics if a residue modulo 2 and characteristic unit do not coincide. Nonprinting fill characters may be inserted to split nonprimitive codeword combinations before transmission. By Theorem 3.7, nonprimitive codeword combinations are to be avoided, if possible. Further investigation is being made.

REFERENCES

1. F. van der Blij, History of the octaves, *Simon Stevin* **34** (1961), 106–125.

2. F. van der Blij and T. A. Springer, The arithmetics of the octaves and of the group G_2, *Nederl. Akad. Wetensch. Proc.* (= *Indag. Math.*) **62A** (1959), 406–418.

3. L. E. Dickson, On quaternions and their generalization and the history of the eight square theorem, *Annals of Math.* (2), **20** (1919), 155–171, 297.

4. A. Hurwitz, Über die Composition der quadratischen Formen von beliebig vielen Variabeln, *Nachr. Gesell. Wiss. Göttingen* (1898), 309–316.

5. P. J. C. Lamont, Arithmetics in Cayley's algebra, *Proc. Glasgow Math. Assoc.* **6** (1963), 99–106.

6. P. J. C. Lamont, Ideals in Cayley's algebra, *Nederl. Akad. Wetensch. Proc.* (= *Indag. Math.*) **66A** (1963), 394–400.

7. P. J. C. Lamont, Approximation theorems for the group G_2, *Nederl. Akad. Wetensch. Proc.* (= *Indag. Math.*) **67A** (1964), 187–192.

8. P. J. C. Lamont, Factorization and arithmetic functions for orders in composition algebras, *Glasgow Math. J.* **14** (1973), 86–95.

9. P. J. C. Lamont, The number of Cayley integers of given norm, *Proc. Edinburgh Math. Soc.* **25** (1982), 101–103.

10. P. J. C. Lamont, Computer generated natural inner automorphisms of Cayley's algebra, *Glasgow Math. J.* **23** (1982), 187–189.

11. P. J. C. Lamont, The nonexistence of a factorization formula for Cayley numbers, *Glasgow Math. J.* **24** (1983), 131–132.

12. R. A. Rankin, On representations of a number as a sum of squares and certain related identities, *Proc. Camb. Phil. Soc.* **41** (1945), 1–11.

13. R. A. Rankin, A certain class of multiplicative functions, *Duke Math. J.* **13** (1946), 281–306.

14. O. Taussky, Sums of squares, *Amer. Math. Monthly* **77** (1970), 805–830.

15. D. Welsh, *Codes and Cryptography* (Oxford, 1988).

DEPARTMENT OF COMPUTER SCIENCE
COLLEGE OF APPLIED SCIENCES
WESTERN ILLINOIS UNIVERSITY
MACOMB, ILLINOIS 61455
U.S.A.