Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 369–376*

Universal Codes and Unimodular Lattices

par Robin CHAPMAN et Patrick SOLÉ

Résumé. Les codes résidus quadratiques binaires de longueur $p+1$ produisent par construction B et bourrage des réseaux de type II comme le réseau de Leech. Récemment, il a été prouvé que les codes résidus quadratiques quaternaires produisent les mêmes réseaux par construction A modulo 4. Nous montrons de manière directe l' équivalence des deux constructions pour $p \leq 31$. En dimension 32 nous obtenons un réseau extrémal de type II qui n'est pas isomètre au réseau de Barnes-Wall BW_{32}. On considère également l'équivalence entre construction B modulo 4 plus bourrage et construction A modulo 8. En dimension 48 elles conduisent toutes deux à une nouvelle description du réseau extrémal de type II appelé P_{48q}.

Abstract. Binary quadratic residue codes of length $p+1$ produce via construction B and density doubling type II lattices like the Leech. Recently, quaternary quadratic residue codes have been shown to produce the same lattices by construction A modulo 4. We prove in a direct way the equivalence of these two constructions for $p \leq 31$. In dimension 32, we obtain an extremal lattice of type II not isometric to the Barnes-Wall lattice BW_{32}. The equivalence between construction B modulo 4 plus density doubling and construction A modulo 8 is also considered. In dimension 48 they both led to a new description of the extremal type II lattice P_{48q}.

1. Introduction

In [2], Bonnecaze, Solé and Calderbank introduce for primes $p \equiv \pm 1 \pmod 8$, codes $\widehat{\mathcal{Q}}$ and $\widehat{\mathcal{N}}$, the *universal extended quadratic residue codes*, of length $p+1$ over the 2-adic integers Z_{2^∞}. For positive integers s they consider their reductions $\widehat{\mathcal{Q}}_{2^s}$ and $\widehat{\mathcal{N}}_{2^s}$ modulo 2^s; $\widehat{\mathcal{Q}}_2$ and $\widehat{\mathcal{N}}_2$ are just the standard binary extended quadratic residue codes, while $\widehat{\mathcal{Q}}_4$ and $\widehat{\mathcal{N}}_4$ are the *quaternary quadratic residue codes*. Given a code C of length n over Z_4

Mots-clés : Quadratic residue codes, Lattices, construction A, construction B, density doubling.
Manuscrit reçu le 30 avril 1996.

define $\Lambda(C)$ as the set of vectors in Z^n which reduce modulo 4 to elements of C. If $p \equiv -1 \pmod 8$ the lattice $\frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$ is even and unimodular ([2] Corollary 4.1); if $p = 7$ it is the E_8 lattice, while if $p = 23$ it is the Leech lattice.

Here we show, by means of an explicit isomorphism, that if $p \equiv -1 \pmod 8$ and $p \leq 31$ then $\frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$ is isometric to a lattice $L(\widehat{\mathcal{Q}}_2)$ constructed from the binary quadratic residue code in a manner (construction B plus density doubling) generalizing the original construction of the Leech lattice. If $p = 23$ this yields a short proof of what is perhaps the simplest construction of the Leech lattice [2]. If $p = 31$ this, combined with results of Koch and Venkov, shows that $BSBM_{32}$ introduced in [1] is not isometric to the Barnes-Wall lattice BW_{32} . In section §4 we consider a quaternary analogue of this situation, replacing construction B by construction B modulo 4, and construction A mod 4 by construction A mod 8. We show, inter alia, that P_{48q} can be obtained in the latter way from a quadratic residue code of length 48 over Z_8.

2. The main result

Throughout this section we assume that p is a prime satisfying $p \equiv -1 \pmod 8$. We also fix an integer r such that $r \equiv 1 \pmod 4$, and $r^2 + p \equiv 0 \pmod{32}$. In addition if $p \leq 31$ we will assume that $r^2 + p = 32$. (If $p = 7$, 23 or 31, then $r = 5$, -3 or 1 respectively.)

We first outline a construction of lattices from binary codes of length $p+1$. Consider a self-orthogonal linear subcode C of Z_2^{p+1}, containing the all-ones word. Define $L(C)$ to be the sublattice of Z^{p+1} generated by the following types of vectors:

(1) all vectors of shape $(8\ 0^p)$,
(2) all vectors of shape $(4^2\ 0^{p-1})$,
(3) all vectors of shape $(2^a\ 0^{p+1-a})$ whose support coincides with the support of an element of C,
(4) any vector of shape $(r\ 1^p)$.

This can be recast as the union of two cosets

$$2B(C) \cup ((r\ 1^p) + 2B(C)),$$

of the lattice $2B(C)$ obtained, up to scaling, by construction B applied to C namely

$$B(C) := C + 2P_{p+1} + 4Z^{p+1},$$

with P_{p+1} denoting the parity-check code of length $p+1$. It is clear that $L(C)$ is a lattice, of index $4^{p+1}/|C|$ in Z^{p+1}. If the code C is doubly even, then the norm of each vector in $L(C)$ is divisible by 16. It follows that if C is self-dual and doubly even then the lattice $\frac{1}{\sqrt{8}}L(C)$ is even and unimodular. If C is $\widehat{\mathcal{Q}}_2$ or $\widehat{\mathcal{N}}_2$ then it has these properties. We give four examples of this construction.

p	lattice	reference
7	Gosset	[7]
23	Leech	[6, p.131]
31	BW_{32}	[7, 9]
31	$BSBM_{32}$	[1]

By the *norm* of an element in Euclidean space we mean the square of its length, and the *minimal norm* of a lattice is the least norm of a non-zero element of the lattice. It is easy to see that the minimum norm of $\frac{1}{\sqrt{8}}L(\widehat{\mathcal{Q}}_2)$ is $\min(4, 2\lceil\frac{p+1}{16}\rceil, \frac{1}{2}\mathrm{mw}(\widehat{\mathcal{Q}}_2))$ where $\mathrm{mw}(C)$ is the minimum (Hamming) weight of the code C.

THEOREM 1. *The lattices* $\frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$ *and* $\frac{1}{\sqrt{8}}L(\widehat{\mathcal{Q}}_2)$ *are isometric for* $p \leq 31$.

Proof. Assume $p \leq 31$. We recall the definition of $\widehat{\mathcal{Q}}$ from §III of [2]. Let δ be the square root of $-p$ in Z_{2^∞} with $\delta \equiv -1 \pmod 4$. Note then that $\delta \equiv -r \pmod{16}$. The vectors m_α ($\alpha \in F_p \cup \{\infty\}$) are defined as the rows of the matrix

$$M = \begin{pmatrix} \delta & 1 \cdots 1 \\ -1 & \\ \vdots & W + \delta I \\ -1 & \end{pmatrix}$$

where

$$W_{ij} = \left(\frac{j-i}{p}\right).$$

(The rows and columns of this matrix are labelled in the order $\infty, 0, 1, \dots,$ $p-1$.) The matrix W is called a Jacobsthal matrix , and is instrumental in building Hadamard matrices of Paley type [10, Chap. II]. We collect here the properties that we need

(J1) $JW = WJ = 0$
(J2) $WW^T = pI - J$
(J3) $A := \sum_{i=\square} W_{-i,1} = -1$
(J4) $B := \sum_{i=\square} W_{i,1} = 0$

where J stands for the all-one matrix. See [10, Chap. II, Lemma 7] for proofs of (J1) and (J2). To prove (J3), (J4) observe firstly that by $(J1)$ we have, knowing that -1 is not a quadratic residue, that $A + B = -1$.

Secondly, writing χ for the Jacobi symbol we have

$$B = \frac{1}{2} \sum_{x \in F_p,\, x \neq 0} \chi(1 - x^2)$$

and by the character property of χ

$$B = \frac{1}{2} \sum_{x \in F_p,\, x \neq 0} \chi(1 - x)\chi(1 + x) = 0,$$

the last equality coming from (J2).

The coordinate positions in the code are labelled $\infty, 0, 1, \ldots, p-1$, regarded as elements of the projective line over F_p. The universal extended quadratic residue code is now defined as

$$\widehat{\mathcal{Q}} = \left(\sum_{\alpha \in F_p \cup \{\infty\}} Q_{2^\infty} m_\alpha \right) \cap Z_{2^\infty}^{p+1},$$

where Q_{2^∞} is the field of 2-adic numbers. A similar definition holds for $\widehat{\mathcal{N}}$ with $W_{i,j}$ replaced by $W_{i,-j}$.

We can now describe $\Lambda(\widehat{\mathcal{Q}}_4)$ as the set of vectors in Z^{p+1} congruent modulo 4 to elements of $\widehat{\mathcal{Q}}$. Let $n_\alpha \in Z^{p+1}$ be the rows of the matrix

$$N = \begin{pmatrix} -r & 1 \cdots 1 \\ -1 & \\ \vdots & W - rI \\ -1 & \end{pmatrix}$$

so that for $\alpha \in F_p \cup \{\infty\}$ we have $n_\alpha \equiv m_\alpha \pmod{16}$. Since by (J2) we have $NN^t = 32I$ the matrix $\frac{1}{\sqrt{32}}N$ is orthogonal. We claim that this matrix maps $\frac{1}{\sqrt{8}}L(\widehat{\mathcal{N}}_2)$ to $\frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$. This is equivalent to saying that N maps $\frac{1}{8}L(\widehat{\mathcal{N}}_2)$ to $\Lambda(\widehat{\mathcal{Q}}_4)$. Note that these codes and lattices are preserved by the automorphism σ coming from the permutation $(0\ 1\ 2\ \cdots\ p-1)$ on $F_p \cup \{\infty\}$, and this automorphism maps m_α to $m_{\alpha+1}$ and n_α to $n_{\alpha+1}$. This automorphism is the shift in the cyclic construction of the QR codes. We proceed to show that the images by N of the four types of vectors in construction L above lie in $\Lambda(\widehat{\mathcal{Q}}_4)$.

Since the $n_\alpha \in \Lambda(\widehat{\mathcal{Q}}_4)$, the matrix N takes the coordinate vectors, which lie in $\frac{1}{8}L(\widehat{\mathcal{N}}_2)$, into $\Lambda(\widehat{\mathcal{Q}}_4)$. For convenience let $(a, b; c; d)$ denote the vector with ∞-coordinate a, 0-coordinate b, and generic α-coordinate c, and generic β-coordinate d where α and β are any quadratic residue, and quadratic non-residue respectively. Now

$$\frac{1}{2}(n_\infty + n_0) = \left(\frac{r-1}{2}, \frac{-r-1}{2}; 0; -1\right)$$

which lies in Z^{p+1} and is congruent to $\frac{1}{2}(m_0 - m_\infty)$ modulo 8. Hence $\frac{1}{2}(m_\infty + m_0) \in \Lambda(\widehat{\mathcal{Q}}_4)$. Applying σ it follows that $\frac{1}{2}(m_\infty + m_\alpha) \in \Lambda(\widehat{\mathcal{Q}}_4)$ for all $\alpha \in F_p$, and so $\frac{1}{2}(m_\alpha + m_\beta) \in \Lambda(\widehat{\mathcal{Q}}_4)$ for all $\alpha, \beta \in F_p \cup \{\infty\}$. Hence $\frac{1}{8}vN \in \Lambda(\widehat{\mathcal{Q}}_4)$ for all v of the shape $(4^2\ 0^{p-1})$. We next compute

$$\frac{1}{4}\left(n_\infty + \sum_{j \in Q'} n_j\right) = \left(-\frac{2r+p-1}{8}, -\frac{p+1}{8}; 0; -\frac{r-1}{4}\right)$$

where Q' is the set of quadratic non-residues modulo p. The last coordinates estimates come from (J3), (J4). Again this has integer coordinates, and is congruent modulo 4 to $\frac{1}{4}(m_\infty + \sum_{j=\Box} m_j)$, so this vector lies in $\Lambda(\widehat{\mathcal{Q}}_4)$. It follows that

$$\frac{1}{4}\left(n_\infty + \sum_{j \in Q'} n_{j+k}\right) \in \Lambda(\widehat{\mathcal{Q}}_4)$$

for each $k \in F_p$. But $\widehat{\mathcal{N}}_2$ is generated by the vectors whose supports are the sets $\{\infty\} \cup (k + Q')$. ([2, p.370, III. A.]). It follows that if v has the shape $(2^a\ 0^{p+1-a})$ and whose support is the same as that of an element of $\widehat{\mathcal{N}}_2$, then $\frac{1}{8}vN \in \Lambda(\widehat{\mathcal{Q}}_4)$. Finally

$$\frac{1}{8}\left(rn_\infty + \sum_{j \in F_p} n_j\right) = (-4, 0; 0; 0) \in \Lambda(\widehat{\mathcal{Q}}_4)$$

and so $\frac{1}{8}(r, 1; 1; 1)N \in \Lambda(\widehat{\mathcal{Q}}_4)$. Hence $\frac{1}{8}L(\widehat{\mathcal{N}}_2)N \subseteq \Lambda(\widehat{\mathcal{Q}}_4)$, and comparing determinants we see that $\frac{1}{8}L(\widehat{\mathcal{N}}_2)N = \Lambda(\widehat{\mathcal{Q}}_4)$. Since $L(\widehat{\mathcal{Q}}_2)$ and $L(\widehat{\mathcal{N}}_2)$ are isometric the Theorem follows. $\Box$

3. Application to the cases of $p = 23, 31$.

If $(a_1, \ldots, a_n)$ is an element of a code over Z_4, then its *Euclidean weight* is $w(a_1) + \cdots + w(a_n)$ where

$$w(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a = \pm 1, \\ 4 & \text{if } a = 2. \end{cases}$$

The *minimum Euclidean weight* $\text{mew}(C)$ of a code C over Z_4 is the least Euclidean weight of its non-zero elements. If C is a linear code then the minimum norm of $\Lambda(C)$ is $\min(16, \mathrm{mew}(C))$. For $p = 23$ and $p = 31$, the minimum norm of $L(\widehat{\mathcal{N}_2})$ is 32, and so the minimum norm of $\Lambda(\widehat{\mathcal{Q}}_4)$ is 16. Hence $\mathrm{mew}(\widehat{\mathcal{Q}}_4) \geq 16$. In [2] this is proved in a more elaborate way for $p = 23$.

In [8] Koch and Venkov show that for the five non-isomorphic doubly even self-dual binary codes $C_1, \dots, C_5$ of length 32, the lattices $L(C_1), \dots, L(C_5)$ are all non-isometric. We can take $C_1 = \widehat{\mathcal{Q}}_2$, and C_2 to be the Reed-Muller code $RM(2,5)$. Since $L(RM(2,5))$ is isometric to the Barnes-Wall lattice BW_{32} [9], it follows that $\frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$ for $p = 31$ is not isometric to BW_{32}, confirming a conjecture of [1]. It is known that there are only two unimodular lattices in dimension 32 with minimal norm 4 and an automorphism of order 31 [12]. From the results of [1] and of the current paper we can infer than both can be constructed by construction A mod 4 applied to an extended quaternary cyclic code: the quaternary Reed-Muller code $QRM(2,5)$ in the case of BW_{32} and the extended quadratic residue code $\widehat{\mathcal{Q}}_4$ in the case of $BSBM_{32} := \frac{1}{2}\Lambda(\widehat{\mathcal{Q}}_4)$. Both lattices also appear in [11, 4].

4. Quaternary Analogue

We assume in this § that $p \geq 47$ is a prime $\equiv -1 \pmod 8$, and that the integer $r \equiv 1 \pmod 4$ satisfies

$$r^2 + p = 96 = 16.6,$$

if $p = 47, 71$ and

$$r^2 + p = 128 = 16.8.$$

if $p = 79, 103, 127$. The corresponding values of r are $r = -7, 5$ in first case and $r = -7, 5, 1$ in the second. For a quaternary code C of length $p+1$ we define

$$B_4(C) := C + 4P_{p+1} + 8Z^{p+1},$$

and

$$L_4(C) := 2B_4(C) \cup ((r\ 1^p) + 2B_4(C)).$$

For an octonary code C_8 of length $p+1$, we define

$$\Lambda_4(C_8) = C_8 + 8Z^{p+1}.$$

We have the following analogue of Theorem 1:

THEOREM 2. *The lattices* $\frac{1}{4}L_4(\widehat{\mathcal{Q}}_4)$ *and* $\frac{1}{\sqrt{8}}\Lambda_4(\widehat{\mathcal{Q}}_8)$ *are isometric for* $p = 47$, *71, 79, 103, 127.*

The proof is analogous to the proof of Theorem 1 and is omitted.

COROLLARY 1. *For* $p = 47$ *the lattice* $\frac{1}{\sqrt{8}}\Lambda(\widehat{\mathcal{Q}}_8)$ *has norm* 6, *and the code* $\widehat{\mathcal{Q}}_8$ *has euclidean minimum weight* 48.

Proof. Follows from the preceding theorem by noticing that $\widehat{\mathcal{Q}}_4$ has euclidean minimum weight 24 [1, 11, 5]. $\square$

The lattice $L_4(\widehat{\mathcal{Q}}_4)$ was considered in [3] and is isometric to P_{48q}. Adopting the definition of P_{48q} in §7.7 of [6], the orthogonal matrix

$$\frac{1}{\sqrt{96}}\begin{pmatrix} -7 & 1 \cdots 1 \\ -1 & \\ \vdots & W-7I \\ -1 & \end{pmatrix}$$

takes P_{48q} to $L_4(\widehat{\mathcal{N}_4})$ (which is isometric to $L_4(\widehat{\mathcal{Q}}_4)$) by a similar argument to Theorem 1. Similarly it is tantamount to conjecture that the conjectural extremal type II lattice of dimension 80 of example 3 of [13] is taken by

$$\frac{1}{\sqrt{128}}\begin{pmatrix} -7 & 1 \cdots 1 \\ -1 & \\ \vdots & W-7I \\ -1 & \end{pmatrix}$$

into $L_4(\widehat{\mathcal{N}_4})$.

5. Conclusion

It would be interesting to lift the remaining three Conway-Pless codes over Z_4 and obtain by construction A_4 the three remaining zero-defect lattices of the Koch-Venkov classification. Similarly the construction of P_{48q} by construction B_3 applied to ternary QR codes and density doubling [6, p.149] suggests a construction modulo 6. Eventually, quaternary double circulant codes which produce an even extremal unimodular lattice in dimension 40 [5] should be amenable to a similar analysis.

6. Acknowledgments

The work described in this paper was done when both authors were Visiting Fellows at the School of Mathematics, Physics, Computing and Electronics at Macquarie University. The first author would like to thank Gerry Myerson for his kind invitation. The second author would like to thank Peter Pleasants for his kind invitation and Macquarie University for two years' hospitality.

REFERENCES

[1] A. Bonnecaze, P. Solé, C. Bachoc, B. Mourrain,'Type II Quaternary Codes' IEEE Trans. Inform. Theory, submitted (1995).

[2] A. Bonnecaze, P. Solé & A. R. Calderbank, 'Quaternary quadratic residue codes and unimodular lattices', *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377, March 1995.

[3] A.R. Calderbank, private communication (1995).

[4] A.R. Calderbank, G. MacGuire, P.V. Kumar, T. Helleseth, Cyclic Codes over Z_4, Locator polynomials, and Newton identities, preprint (1995).

[5] A. R. Calderbank, N. J. A. Sloane, 'Double Circulant Codes over Z_4 and Unimodular Lattices', J. of Algebraic Combinatorics, submitted.

[6] J. H. Conway & N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[7] G. D. Forney, 'Coset Codes II: Binary Lattices and related codes', IEEE Trans. Information Th. IT-34 (1988) 1152-1187.

[8] H. Koch & B.B. Venkov, Ueber Ganzhalige Unimodulare Euklidische Gitter, Crelle 398 (1989) 144-168.

[9] P. Loyer, P. Solé, 'Les Réseaux BW32 et U32 sont équivalents', J. de Th. des Nombres de Bordeaux 6 (1994) 359-362.

[10] F. J. MacWilliams, N.J.A. Sloane, *The theory of error correcting codes* North-Holland (1977).

[11] V. Pless, Z. Qian, 'Cyclic Codes and Quadratic Residue Codes over Z_4 ', IEEE Trans. Information Theory submitted.

[12] H-G. Quebbemann, 'Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung', Crelle 326 (1981) 158-170.

[13] R. Schulze-Pillot, 'Quadratic Residue Codes and Cyclotomic lattices', Arch. Math., Vol. 60 (1993) 40-65.

Robin CHAPMAN
Department of Mathematics
University of Exeter
EX4 4QE
U.K.
rjc@maths.exeter.ac.uk

Patrick SOLÉ
CNRS-I3S
BP 145
06903 Sophia Antipolis cedex
France
sole@alto.unice.fr