DEMONSTRATIO MATHEMATICA
Vol. XXXVIII No 2 2005

Dietmar Dorninger, Helmut Länger, Maciej Mączyński

ON RING-LIKE STRUCTURES RELATED TO SYMMETRIC CRYPTOSYSTEMS

Abstract. The aim of this paper is to study cryptographic systems defined as algebras $(A, +_\alpha, +_\beta, p, s)$ of type $(2,2,0,0)$ satisfying the axiom $(x+_\alpha p)+_\beta s = x$ for all $x \in A$. Some standard and non-standard examples of such systems are given. In particular, we study the systems for which $+_\alpha = +_\beta = +$ and $p = s$ where the operation $+$ is the addition operation of a generalized Boolean quasiring (GBQR). We investigate the structure of these algebras revealing their relation to orthomodular lattices and characterize the systems for which s (which is interpreted as coding and decoding key) commutes with all elements of A. By applying direct products to cryptographic algebras one can construct complicated cryptographic systems which may be of importance for practical use. (Then the keys are sequences whose components may be selected at random like in an XOR[2] protocol.)

1. Introduction

Within a cryptographic protocol let x, p and s denote messages, public keys and secrete keys, respectively. Denoting the outcome of the encryption and decryption procedures by $x +_\alpha p$ and $x +_\beta s$, respectively, the element x has to be recovered by computing $(x +_\alpha p) +_\beta s$. This motivates the following

DEFINITION 1.1. *A* cryptographic algebra *is an algebra* $\mathcal{A} = (A, +_\alpha, +_\beta, p, s)$ *of type* $(2, 2, 0, 0)$ *satisfying* $(x +_\alpha p) +_\beta s = x$ *for all* $x \in A$. $\mathcal{A}$ *is called* symmetric *if* $p = s$; *otherwise it is called* nonsymmetric. *If* $+_\alpha$ *and* $+_\beta$ *coincide we write* $+$ *instead of* $+_\alpha, +_\beta$. *If* p *and* s *coincide we write* s *instead of* p, s. *If* $(x + s) + s = x$ *for all* $x, s \in A$, *we call* $(A, +)$ *a* completely symmetric cryptographic algebra.

1991 *Mathematics Subject Classification*: 08A62, 16Y99, 51E14.

Key words and phrases: Cryptographic algebra, generalized Boolean quasiring (GBQR), completely symmetric cryptographic GBQR, finite incidence structure, symmetric cryptographic GBQR.

[1] Research supported by the Partnership Agreement between the Vienna University of Technology and the Warsaw University of Technology.

[2] Exclusive-or operation.

We start by giving two well-known and a new example for cryptographic algebras in order to motivate our definition. (For notions and concepts of cryptography used in the following we refer to [9].) Our next step will then be to introduce a whole new class of such algebras.

EXAMPLE 1.1. The Vernam One-time Pad (a completely symmetric cryptosystem)

The additive group $\mathcal{A}$ of the two-element Boolean ring is a completely symmetric cryptographic algebra and hence the same is true for the direct power $\mathcal{A}^n$. Every element of A^n may serve as the private as well as the public key of an individual participant.

EXAMPLE 1.2. RSA (an asymmetric cryptosystem)

Let $1, \ldots, n$ be participants with public keys (m_i, p_i) and private keys $s_i, i = 1, \ldots, n$, ($m_i = a_i b_i$, a_i, b_i different prime numbers, $p_i < m_i$ a positive integer relative prime to $(a_i - 1)(b_i - 1)$ and s_i the unique positive integer $< \operatorname{lcm}(a_i - 1, b_i - 1)$ satisfying $s_i p_i \equiv 1 \bmod \operatorname{lcm}(a_i - 1, b_i - 1)$). For $j \in \{1, \ldots, n\}$ define $A_j := \{0, \ldots, m_i - 1\}$ and $x +_j y :\equiv x^y \bmod m_j$ for all $x, y \in A_j$. Then $(x +_j p_j) +_j s_j = x$ for all $x \in A_j$, i. e. $\mathcal{A}_j := (A_j, +_j, p_j, s_j)$ is a cryptographic algebra. Moreover, the direct product of the algebras $\mathcal{A}_1, \ldots, \mathcal{A}_n$ is also a cryptographic algebra which can then serve as the context for the whole RSA-system.

EXAMPLE 1.3. (Cryptosystems generated by character tables of finite point symmetry groups of molecules)

Let n be a positive integer, A denote the set of all $n \times n$-matrices over $\mathbf{R}$ and binary operations $+_\alpha$ and $+_\beta$ on A be defined as follows:

$$x +_\alpha y := xy \text{ and}$$
$$x +_\beta y := \begin{cases} xy^{-1} & \text{if } |y| \neq 0 \\ O & \text{otherwise} \end{cases}$$

$(x, y \in A)$. Further let s be a fixed regular $n \times n$-matrix over $\mathbf{R}$. Then $(A, +_\alpha, +_\beta, s)$ is a symmetric cryptographic algebra. In particular, we may consider s as the $n \times n$-matrix of the characters of the symmetry group $\mathcal{G}$ of a molecule M. It is known that the columns of this matrix correspond to the conjugacy classes of $\mathcal{G}$ and the rows to the irreducible representations of $\mathcal{G}$. We denote the cardinality of the conjugacy class corresponding to the j-th column of s by N_j, $j = 1, \ldots, n$, and the irreducible representation of $\mathcal{G}$ corresponding to the i-th row of s by Γ_i, $i = 1, \ldots, n$. Then it is known from the representation theory of finite symmetry groups that $|s| \neq 0$ and with $h := \sum_{j=1}^{n} N_j$ for the order of $\mathcal{G}$

$$s^{-1} = \left(\frac{N_j}{h} s_{ij}\right)^T$$

(this is in fact the orthogonality theorem for characters). If

$$x := \begin{pmatrix} x_1 & \dots & x_n \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

corresponding to the representation

$$\Gamma = x_1\Gamma_1 \oplus \ldots \oplus x_n\Gamma_n \tag{1}$$

(where $\oplus$ denotes the direct sum) then xs corresponds to the characters of Γ. If Γ is interpreted as a composed vibration of M then xs is the code of the vibration Γ in terms of the characters of Γ. We may decode the vibration by using the matrix s and computing $(xs)s^{-1} = x$. Hence every molecule can be interpreted as providing a key s for coding and decoding the vibrations. Let us recall that the characters of the vibration Γ can be calculated from the structure of the molecule without knowing decomposition (1). Then we decode it by applying the character table s and we obtain decomposition (1).

REMARK 1.1. *If $\mathcal{A}$ is a cryptographic algebra then $x \mapsto x +_\alpha p$ is injective and $x \mapsto x +_\beta s$ is surjective, hence if $\mathcal{A}$ is finite then both mappings are bijective and therefore polynomial permutations in the sense of* [8]. *In case of symmetric cryptographic algebras with $+_\alpha = +_\beta$, $x \mapsto x + s$ is already bijective and for completely symmetric cryptographic algebras $x \mapsto x + a$ is bijective for any $a \in A$, i. e. the mappings $x \mapsto x + s$ and $x \mapsto x + a$ are polynomial permutations.*

REMARK 1.2. *In order to obtain better structural results about completely symmetric cryptographic algebras and thus better ways of constructing these algebras we have restricted the definition of completely symmetric cryptographic algebras to the case $+_\alpha = +_\beta$. Moreover, if for a symmetric cryptographic algebra $(A, +_\alpha, +_\beta, s)$ it holds that $(x +_\alpha s) +_\alpha s = x$ for all $x, s \in A$, then $(x +_\alpha s) +_\beta s = x$ for all $x, s \in A$ implies $x +_\alpha s = x +_\beta s$ for all $x, s \in A$ as one can see immediately by substituting $x +_\alpha s$ for x in $(x +_\alpha s) +_\beta s = x$.*

Any algebra whose type is extended by nullary operations in such a way that the extended type includes the type $(2, 2, 0, 0)$ or $(2, 0, 0)$, respectively, can be considered as a candidate for a cryptographic algebra. In this paper our choice will be the variety of generalized Boolean quasirings (GBQRs), which are generalizations of Boolean rings arising in a natural way when extending the correspondence between Boolean algebras and Boolean rings to bounded lattices with an involutory antiautomorphism.

GBQRs are defined as follows (for this definition and further properties cf. [1] – [6]):

DEFINITION 1.2. *An algebra* $(R, +, \cdot)$ *of type* $(2, 2)$ *is called a* generalized Boolean quasiring (GBQR) *if there exist* $0, 1 \in R$ *such that* (1) – (8) *hold for all* $x, y, z \in R$*:*

(1) $x + y = y + x$,

(2) $0 + x = x$,

(3) $(xy)z = x(yz)$,

(4) $xy = yx$,

(5) $xx = x$,

(6) $x0 = 0$,

(7) $x1 = x$ *and*

(8) $1 + (1 + xy)(1 + x) = x$.

(The elements 0 *and* 1 *of a* GBQR *are uniquely determined.) Omitting axiom* (1) *and considering* $+$ *as a partial binary operation* $\oplus$ *on* R *defined on* $\{0, 1\} \times R$*, one obtains a partial algebra called a* partial GBQR (pGBQR).

The algebras $(R, \oplus, \cdot)$ are in one-to-one correspondence with bounded lattices $(L, \vee, \wedge, ^*, 0, 1)$ with an involutory antiautomorphism * by means of the definitions

$$x \vee y := 1 \oplus (1 \oplus x)(1 \oplus y)$$
$$x \wedge y := xy$$
$$x^* := 1 \oplus x$$

and

$$0 \oplus x := x$$
$$1 \oplus x := x^*$$
$$xy := x \wedge y,$$

respectively. For a given GBQR $\mathcal{R}$ we write $\mathbf{L}(\mathcal{R})$ for the associated lattice.

A pGBQR $(R, \oplus, \cdot)$ can be extended to a GBQR $(R, +, \cdot)$ by defining $0 + x = x + 0 := 0 \oplus x$, $1 + x = x + 1 := 1 \oplus x$ for all $x \in R$ and arbitrarily setting up $x + y = y + x$ for all $x, y \in R \setminus \{0, 1\}$.

Two canonical examples for extensions of $\oplus$ are

$$x +_1 y = 1 \oplus (1 \oplus x(1 \oplus y))(1 \oplus (1 \oplus x)y) \text{ and}$$
$$x +_2 y = (1 \oplus (1 \oplus x)(1 \oplus y))(1 \oplus xy)$$

which both represent the symmetric difference in the Boolean algebras which correspond to Boolean rings.

For all $x, y \in R$ we have $x +_1 y \leq x +_2 y$, where $\leq$ is defined in $\mathbf{L}(\mathcal{R})$. If for an extension $+$ of $\oplus$ it holds that $x +_1 y \leq x + y \leq x +_2 y$ for all $x, y \in R$, we will denote this fact by simply writing $+_1 \leq + \leq +_2$.

Because of the many possibilities to construct GBQRs these algebras (with respect to their operation $+$) qualify as candidates for cryptographic algebras.

DEFINITION 1.3. *A* cryptographic GBQR *is an algebra* $\mathcal{R} = (R, +_\alpha, +_\beta, \cdot, p, s)$ *of type* $(2, 2, 2, 0, 0)$ *such that* $(R, +_\alpha, \cdot)$ *and* $(R, +_\beta, \cdot)$ *are* GBQRs *and* $\mathcal{R}' = (R, +_\alpha, +_\beta, p, s)$ *is a cryptographic algebra.* $\mathcal{R}$ *is called* symmetric *or* non-symmetric *if* $\mathcal{R}'$ *has the corresponding property. If* $+_\alpha$ *and* $+_\beta$ *coincide, we write* $+$ *instead of* $+_\alpha, +_\beta$*. If* p *and* s *coincide, we write* s *instead of* p, s*. A* GBQR $(R, +, \cdot)$ *is called a* completely symmetric cryptographic GBQR *if* $(R, +)$ *is a completely symmetric cryptographic algebra, i. e. if* $(x+y)+y = x$ *for all* $x, y \in R$.

EXAMPLE 1.4. The operation tables

$+_\alpha$	0	a	a^*	b	b^*	1
0	0	a	a^*	b	b^*	1
a	a	0	1	b	b^*	a^*
a^*	a^*	1	0			a
b	b	b		0	1	b^*
b^*	b^*	b^*		1	0	b
1	1	a^*	a	b^*	b	0

,

$+_\beta$	0	a	a^*	b	b^*	1
0	0	a	a^*	b	b^*	1
a	a	0	1	b	b^*	a^*
a^*	a^*	1	0			a
b	b	b		0	1	b^*
b^*	b^*	b^*		1	0	b
1	1	a^*	a	b^*	b	0

and

$\cdot$	0	a	a^*	b	b^*	1
0	0	0	0	0	0	0
a	0	a	0	0	0	a
a^*	0	0	a^*	0	0	a^*
b	0	0	0	b	0	b
b^*	0	0	0	0	b^*	b^*
1	0	a	a^*	b	b^*	1

(where the empty places can be filled arbitrarily such that the corresponding operation table is symmetric with respect to the main diagonal) define a symmetric cryptographic GBQR $(\{0, a, a^*, b, b^*, 1\}, +_\alpha, +_\beta, a)$.

In the following we study completely symmetric and symmetric cryptographic GBQRs from the algebraic point of view. Nonsymmetric cryptograpghic GBQRs as well as considerations concerning the cryptographic strength of cryptographic GBQRs will be the subject of further investigations.

2. Completely symmetric cryptographic GBQRs

A completely symmetric cryptographic GBQR is characterized by the equation $(x+y)+y=x$ for all $x, y \in R$. Immediate consequences of this equation are $x+x=0$ and $x+x^*=1$ for all $x \in R$.

We recall that for an arbitrary GBQR $(R,+,\cdot)$ with $+_1 \leq + \leq +_2$

$$\begin{aligned}
&x \leq y \Rightarrow x+y=x^* \wedge y, \\
&x \geq y \Rightarrow x+y=x \wedge y^*, \\
&x \perp y \Rightarrow x+y=x \vee y \text{ and} \\
&x^* \perp y^* \Rightarrow x+y=x^* \vee y^*
\end{aligned}$$

where $x \perp y$ is defined by $x \leq y^*$ $(x, y \in R)$. (These implications hold because they are true for $+_1$ and $+_2$ instead of $+$. The operations $\vee$, $\wedge$, * and the relations $\leq$ and $\perp$ relate to the corresponding lattice $\mathbf{L}(\mathcal{R})$ and will always be used in this sense in the following.)

Let $\mathcal{R}=(R,+,\cdot)$ be an arbitrary GBQR satisfying $+_1 \leq + \leq +_2$ and assume $\mathbf{L}(\mathcal{R})$ to be orthomodular. Then it can be easily checked that $(x+y)+y=x$ for all those $x, y \in R$ which satisfy one of the relations $x \leq y$, $x \geq y$, $x \perp y$ or $x^* \perp y^*$.

Observing that a bounded lattice with an involutory antiautomorphism which satisfies the orthomodular law is an ortholattice we prove:

LEMMA 2.1. *Let $\mathcal{R}=(R,+,\cdot)$ be an arbitrary* GBQR *with the property that $x+y=x^* \vee y^*$ for $x, y \in R$ with $x^* \perp y^*$. Then*

$$(x+y)+y=x \text{ for all } x, y \in R \text{ with } y \geq x^* \tag{2}$$

if and only if $\mathbf{L}(\mathcal{R})$ *is orthomodular.*

Proof. For all $x, y \in R$ with $x^* \perp y^*$, i. e. with $y \geq x^*$, we have

$$(x+y)+y=(x^* \vee y^*)+y=(x^* \vee y^*)^* \vee y^*=(x \wedge y) \vee y^*.$$

Since $x^* \perp y^*$ is equivalent to $y^* \leq x$ and orthomodularity of $\mathbf{L}(\mathcal{R})$ can be characterized by $y^* \leq x \Rightarrow x=y^* \vee (x \wedge y)$, $\mathbf{L}(\mathcal{R})$ is orthomodular if and only if $\mathcal{R}$ satisfies (2). •

THEOREM 2.1. *If $\mathcal{R}=(R,+,\cdot)$ is a completely symmetric cryptographic* GBQR *satisfying $+_1 \leq + \leq +_2$ then $\mathbf{L}(\mathcal{R})$ is orthomodular. On the other* *hand, given an orthomodular lattice the partial operation* $\oplus$ *of the associated* pGBQR *cannot always be extended to a full operation* $+$ *such that the corresponding* GBQR *is a completely symmetric cryptographic* GBQR.

Proof. Given a completely symmetric cryptographic GBQR $\mathcal{R} = (R, +, \cdot)$ with $+_1 \le + \le +_2$ and $x + y = x^* \vee y^*$ for $x, y \in R$ with $x^* \perp y^*$, $\mathbf{L}(\mathcal{R})$ is orthomodular according to Lemma 2.1.

To prove the second part of the theorem suppose that there exists a completely symmetric cryptographic GBQR the corresponding lattice of which is the six-element orthomodular lattice $\mathcal{L}$. Then one can obtain a contradiction by appropriately checking the equation $(x + y) + y = x$ for various possibilities for the outcome of $a + b$ where a, b are two different atoms of $\mathcal{L}$ which are not orthogonal. •

REMARK 2.1. *The lattice corresponding to a completely symmetric cryptographic* GBQR $(R, +, \cdot)$ *satisfying* $+_1 \le + \le +_2$ *need not be a Boolean algebra, as can be seen by means of the class of* GBQRs *definied in Example 2.1.*

EXAMPLE 2.1. Let (P, L) be a finite incidence structure of points (set P with $|P| > 1$) and lines (set $L \subseteq 2^P$) such that $|x| = 3$ for all $x \in L$ and that for every pair x, y of different elements of P there exists exactly one $f(x, y) \in L$ with $x, y \in f(x, y)$. For an element $0 \notin P$ we consider the set $A := (P \cup \{0\}) \times \{0, 1\}$ and define binary operations $+$ and $\cdot$ on A by

$$(x,i) + (y,j) := \begin{cases} (0,0) & \text{if } x, y \in P, x = y \text{ and } i = j, \\ (0,1) & \text{if } x, y \in P, x = y \text{ and } i \neq j, \\ (z, i+j) & \text{if } x, y \in P, x \neq y \text{ and } f(x,y) = \{x, y, z\}, \\ (y,j) & \text{if } (x,i) = (0,0), \\ (y, 1-j) & \text{if } (x,i) = (0,1), \\ (x,i) & \text{if } (y,j) = (0,0) \text{ and} \\ (x, 1-i) & \text{if } (y,j) = (0,1) \end{cases}$$

(where $i + j$ is to be taken modulo 2) and

$$(x,i) \cdot (y,j) := \begin{cases} (y,j) & \text{if } (x,i) = (0,1), \\ (x,i) & \text{if } (y,j) = (0,1), \\ (x,i) & \text{if } (x,i) = (y,j) \text{ and} \\ (0,0) & \text{otherwise} \end{cases}$$

$((x,i), (y,j) \in A)$. Then $(A, +, \cdot)$ is a completely symmetric cryptographic GBQR satisfying $+_1 \le + \le +_2$, the corresponding lattice of which is the $(2|P| + 2)$-element orthomodular lattice of length 2 with $P \times \{0, 1\}$ as set of atoms, which is not Boolean. Trivial examples for (P, L) are

$$\begin{aligned}&(\{1,2,3\},\{\{1,2,3\}\}),\\&(\{1,2,3,4,5,6,7\},\{\{1,2,5\},\{1,3,7\},\{1,4,6\},\{2,3,6\},\{2,4,7\},\{3,4,5\},\\&\qquad\{5,6,7\}\})\\&\qquad\text{and}\\&(\{1,2,3,4,5,6,7,8,9\},\{\{1,2,3\},\{1,4,7\},\{1,5,9\},\{1,6,8\},\{2,4,9\},\\&\qquad\{2,5,8\},\{2,6,7\},\{3,4,8\},\{3,5,7\},\{3,6,9\},\{4,5,6\},\{7,8,9\}\}).\end{aligned}$$

A necessary condition for the existence of a geometry (P, L) is that $|P|(|P|-1) = 6|L|$. From this it follows $|P| \equiv 0$ or 1 or 3 or $4 \bmod 6$.

However, if $+ = +_1$ or $+ = +_2$ then we end up with a Boolean ring.

THEOREM 2.2. *A* GBQR $\mathcal{R} = (R, +, \cdot)$ *is a completely symmetric cryptographic* GBQR *satisfying* $+ = +_1$ *or* $+ = +_2$ *if and only if it is a Boolean ring.*

Proof. Assume $\mathcal{R}$ to be a completely symmetric cryptographic GBQR satisfying $+ = +_1$ or $+ = +_2$. According to Theorem 2.1, $\mathbf{L}(\mathcal{R})$ is orthomodular. If $+ = +_1$ then

$$\begin{aligned}x \vee y &= ((x +_1 y) +_1 y) \vee y =\\&= (((x \wedge y^*) \vee (x^* \wedge y)) \wedge y^*) \vee ((x^* \vee y) \wedge (x \vee y^*) \wedge y) \vee y =\\&= (x \wedge y^*) \vee y\end{aligned}$$

for all $x, y \in R$, and if $+ = +_2$ then

$$\begin{aligned}x \wedge y^* &= ((x +_2 y) +_2 y) \wedge y^* =\\&= (((x \vee y) \wedge (x^* \vee y^*)) \vee y) \wedge ((x^* \wedge y^*) \vee (x \wedge y) \vee y^*) \wedge y^* =\\&= (x \vee y) \wedge y^*\end{aligned}$$

for all $x, y \in R$. Hence any two elements of $\mathbf{L}(\mathcal{R})$ commute showing that $\mathbf{L}(\mathcal{R})$ is a Boolean algebra which together with $+ = +_1$ or $+ = +_2$ implies that $\mathcal{R}$ is a Boolean ring. The rest of the proof is obvious. •

3. Symmetric cryptographic GBQRs

THEOREM 3.1. *Every cryptographic* GBQR $(R, +_\alpha, +_\beta, \cdot, p, s)$ *satisfying* $+_1 \leq +_\alpha \leq +_2$ *is symmetric.*

Proof. Let $\vee_\alpha$ and $\wedge_\alpha$ denote the lattice operations of $\mathbf{L}((R, +_\alpha, \cdot))$. Then

$$\begin{aligned}p &= (p +_\alpha p) +_\beta s = (((p +_\alpha p) +_\alpha p) +_\beta s) +_\beta s =\\&= (((p \wedge_\alpha p^*) +_\alpha p) +_\beta s) +_\beta s = (((p \wedge_\alpha p^*)^* \wedge_\alpha p) +_\beta s) +_\beta s =\\&= (((p^* \vee_\alpha p) \wedge_\alpha p) +_\beta s) +_\beta s = (p +_\beta s) +_\beta s =\\&= ((0 +_\alpha p) +_\beta s) +_\beta s = 0 +_\beta s = s.\end{aligned}$$

•

COROLLARY 3.1. *If $\mathcal{R} = (R, +, \cdot)$ is a* GBQR *satisfying $+_1 \leq + \leq +_2$ and for every $p \in R$ there exists an $s \in R$ such that $(x + p) + s = x$ for all $x \in R$ then $\mathcal{R}$ is a completely symmetric cryptographic* GBQR.

DEFINITION 3.1. *For every lattice $(L, \vee, \wedge, ^*)$ with an involutory antiautomorphism we define a binary relation* C *on L by*

$$x \,\mathrm{C}\, y \text{ if and only if } x = (x \wedge y) \vee (x \wedge y^*).$$

We observe that if $a \in L$ and $x \,\mathrm{C}\, a$ for all $x \in L$ then

$$x = (x^*)^* = ((x^* \wedge a) \vee (x^* \wedge a^*))^* = (x \vee a^*) \wedge (x \vee a) = (x \vee a) \wedge (x \vee a^*)$$

for all $x \in L$.

LEMMA 3.1. *If $(R, +_\alpha, \cdot)$ and $(R, +_\beta, \cdot)$ are* GBQRs *satisfying $+_1 \leq +_\alpha$, $+_\beta \leq +_2$, $a, s \in R$, $s \wedge s^* = 0$ and $a \,\mathrm{C}\, s$ then $(a +_\alpha s) +_\beta s = a$.*

Proof. Since $s \wedge s^* = 0$ we have $s \vee s^* = 1$ and hence (by using the distributive inequalities)

$$\begin{aligned}
a &= (a \wedge s^*) \vee (a \wedge s) = (a \wedge s^*) \vee (a^* \wedge s \wedge s^*) \vee (a^* \wedge s^* \wedge s) \vee (a \wedge s) \leq \\
&\leq (((a \wedge s^*) \vee (a^* \wedge s)) \wedge s^*) \vee (((a^* \wedge s^*) \vee (a \wedge s)) \wedge s) = \\
&= ((a +_1 s) \wedge s^*) \vee ((a +_2 s)^* \wedge s) \leq ((a +_\alpha s) \wedge s^*) \vee ((a +_\alpha s)^* \wedge s) = \\
&= (a +_\alpha s) +_1 s \leq (a +_\alpha s) +_\beta s \leq (a +_\alpha s) +_2 s = \\
&= ((a +_\alpha s) \vee s) \wedge ((a +_\alpha s)^* \vee s^*) \leq ((a +_2 s) \vee s) \wedge ((a +_1 s)^* \vee s^*) = \\
&= (((a \vee s) \wedge (a^* \vee s^*)) \vee s) \wedge (((a^* \vee s) \wedge (a \vee s^*)) \vee s^*) \leq \\
&\leq (a \vee s) \wedge (a^* \vee s^* \vee s) \wedge (a^* \vee s \vee s^*) \wedge (a \vee s^*) = \\
&= (a \vee s) \wedge (a \vee s^*) = a
\end{aligned}$$

which shows $(a +_\alpha s) +_\beta s = a$. •

THEOREM 3.2. *If $(R, +_\alpha, \cdot)$ and $(R, +_\beta, \cdot)$ are* GBQRs *satisfying $+_1 \leq +_\alpha$, $+_\beta \leq +_2$, $s \in R$ and $x \,\mathrm{C}\, s$ for all $x \in R$ then $(R, +_\alpha, +_\beta, \cdot, s)$ is a cryptographic* GBQR.

Proof. The result follows from Lemma 3.1 by observing that $s \wedge s^* = (0 \vee s) \wedge (0 \vee s^*) = 0$. •

LEMMA 3.2. *Let $(R, +, \cdot)$ be a* GBQR *and $a, s \in R$. Then any single of the following conditions implies $a \,\mathrm{C}\, s$:*

$$\begin{aligned}
&(a +_1 s) +_1 s = a, \\
&(a +_2 s) +_1 s = a, \\
&(a^* +_2 s) +_2 s = a^* \text{ and} \\
&(a^* +_1 s) +_2 s = a^*.
\end{aligned}$$

Proof. Since for $i, j = 1, 2$ one has $(a^* +_{3-i} s) +_{3-j} s = ((a +_i s) +_j s)^*$ the equalities $(a +_i s) +_j s = a$ and $(a^* +_{3-i} s) +_{3-j} s = a^*$ are equivalent. First assume $(a +_1 s) +_1 s = a$. Put

$$b := ((a \wedge s^*) \vee (a^* \wedge s)) \wedge s^* \text{ and}$$
$$c := (a \vee s^*) \wedge s.$$

Then

$$a = (a +_1 s) +_1 s = b \vee ((a^* \vee s) \wedge (a \vee s^*) \wedge s^*) = b \vee e$$

and hence $b, c \leq a$. From this it follows that

$$a \wedge s^* \leq b \leq a \wedge s^* \text{ and}$$
$$a \wedge s \leq c \leq a \wedge s$$

which shows $(a \wedge s^*) \vee (a \wedge s) = b \vee c = a$ proving $a\,\mathrm{C}\,s$.

Now assume $(a +_2 s) +_1 s = a$. Put

$$d := (a \vee s) \wedge s^* \text{ and}$$
$$e := ((a^* \wedge s^*) \vee (a \wedge s)) \wedge s.$$

Then

$$a = (a +_2 s) +_1 s = ((a \vee s) \wedge (a^* \vee s^*) \wedge s^*) \vee e = d \vee e$$

and hence $d, e \leq a$ which yields

$$a \wedge s^* \leq d \leq a \wedge s^* \text{ and}$$
$$a \wedge s \leq e \leq a \wedge s$$

showing $(a \wedge s^*) \vee (a \wedge s) = d \vee e = a$, i. e. $a\,\mathrm{C}\,s$. ●

THEOREM 3.3. *Let $(R, +, \cdot)$ be a* GBQR, *$i, j \in \{1, 2\}$ and $s \in R$. Then $(R, +_i, +_j, \cdot, s)$ is a cryptographic* GBQR *if and only if $x\,\mathrm{C}\,s$ for all $x \in R$.*

Proof. The result follows from Theorem 3.2 and Lemma 3.2. ●

Theorem 3.2 shows that any GBQRs $(R, +_\alpha, \cdot)$ and $(R, +_\beta, \cdot)$ satisfying $+_1 \leq +_\alpha, +_\beta \leq +_2$ defined by means of an ortholattice that contains an element s such that $x\,\mathrm{C}\,s$ for all $x \in R$ can serve as an example of a cryptographic GBQR. (For the structure of such lattices cf. e. g. [7].)

An example of a bounded lattice $(L, \vee, \wedge, ^*, 0, 1)$ with an involutory antiautomorphism that is not an ortholattice and contains an element $s \neq 0, 1$ such that $x\,\mathrm{C}\,s$ for all $x \in L$ is given in Fig. 3.1:

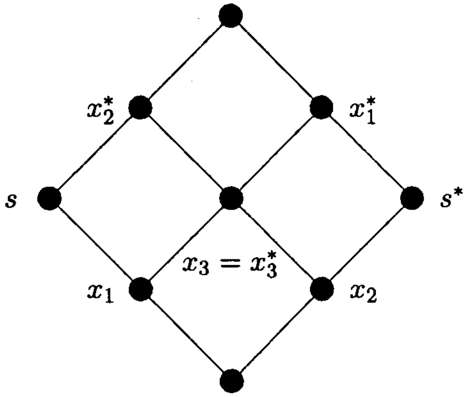

Fig. 3.1

Starting from a bounded lattice $(L, \vee, \wedge, ^*, 0, 1)$ with an involutory antiautomorphism with the property that there exists an element s of L with $x \, \mathrm{C} \, s$ for all $x \in L$ one can obtain different GBQRs by differently extending the operation $\oplus$ to $+_\alpha$ and $+_\beta$, respectively. Performing direct products of (a large number of) copies of small lattices with the appropriate properties and assigning GBQRs to these direct products the direct products of the GBQRs obtained this way can serve for cryptographic purposes. If one needs completely symmetric cryptographic GBQRs one can start with orthomodular lattices like in Example 2.1 or with Boolean algebras.

References

[1] D. Dorninger, H. Länger and M. Mączyński, *The logic induced by a system of homomorphisms and its various algebraic characterizations*, Demonstratio Math. 30 (1997), 215–232.

[2] D. Dorninger, H. Länger and M. Mączyński, *On ring-like structures occurring in axiomatic quantum mechanics*, Österr. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 206 (1997), 279–289.

[3] D. Dorninger, H. Länger and M. Mączyński, *On ring-like structures induced by Mackey's probability function*, Rep. Math. Phys. 43 (1999), 499–515.

[4] D. Dorninger, H. Länger and M. Mączyński, *Lattice properties of ring-like quantum logics*, Intern. J. Theor. Phys. 39 (2000), 1015–1026.

[5] D. Dorninger, H. Länger and M. Mączyński, *Concepts of measures on ring-like quantum logics*, Rep. Math. Phys. 47 (2001), 167–176.

[6] D. Dorninger, H. Länger and M. Mączyński, *Ring-like structures with unique symmetric difference related to quantum logic*, Discuss. Math. General Algebra Appl. 21 (2001), 239–253.

[7] G. Kalmbach, *Orthomodular Lattices*, Academic Press, London 1983.

[8] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam, and Amer. Elsevier, New York, 1973.

[9] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton 1997.
(http://www.cacr.math.uwaterloo.ca/hac/)

Authors' addresses:
Dietmar Dorninger and Helmut Länger
VIENNA UNIVERSITY OF TECHNOLOGY
INSTITUTE OF DISCRETE MATHEMATICS AND GEOMETRY
Wiedner Hauptstraße 8–10
1040 VIENNA, AUSTRIA
E-mail: d.dorninger@tuwien.ac.at and h.laenger@tuwien.ac.at

Maciej Mączyński
WARSAW UNIVERSITY OF TECHNOLOGY
FACULTY OF MATHEMATICS AND INFORMATION SCIENCE
Plac Politechniki 1
00-661 WARSAW, POLAND
E-mail: mamacz@alpha.mini.pw.edu.pl

Received August 27, 2004.