Boolean Gröbner Bases

Yosuke Sato

Department of Mathematical Information Science, Tokyo University of Science, Kagurazaka 1-3, Shinjuku-ku, Tokyo 162-8601, Japan

Shutaro Inoue

Department of Mathematical Information Science, Tokyo University of Science, Kagurazaka 1-3, Shinjuku-ku, Tokyo 162-8601, Japan

Akira Suzuki

Graduate School of Science and Technology, Kobe University, Rokkodai-cho 1-1, Nada-ku, Kobe 657-8501, Japan

Katsusuke Nabeshima

Institute of Socio-Arts and Sciences, The University of Tokushima, Minamijosanjima-cho 2-1, Tokushima 770-8506, Japan

Ko Sakai

Department of Mathematics, University of Tsukuba, Tennodai 1-1-1, Tsukuba 305-8571, Japan

---

Abstract

In recent years, Boolean Gröbner bases have attracted the attention of many researchers, mainly in connection with cryptography. Several sophisticated methods have been developed for the computation of Boolean Gröbner bases. However, most of them only deal with Boolean polynomial rings over the simplest coefficient Boolean ring $\mathbb{GF}_2$. Boolean Gröbner bases for arbitrary coefficient Boolean rings were first introduced by two of the authors almost two decades ago. While the work is not well known among computer algebra researchers, recent active work on Boolean Gröbner bases inspired us to return to their development. In this paper, we introduce our work on Boolean Gröbner bases with arbitrary coefficient Boolean rings.

Key words: Boolean ring, Gröbner bases, Comprehensive Gröbner bases

---

Preprint submitted to Elsevier *22 September 2010*

1. Introduction

Boolean Gröbner bases have been studied by many researchers in recent years, mainly in connection with cryptography (3; 5; 6; 8). Several sophisticated methods have been developed for the computation of Boolean Gröbner bases in computer algebra systems such as Singular (27), Magma (14) and PolyBoRi (19), etc. However, the Boolean Gröbner basis in these works is the Gröbner basis of an ideal in a polynomial ring over the Galois field $\mathbb{GF}_2$, the simplest Boolean ring. Since $\mathbb{GF}_2$ is actually a field, such a Boolean Gröbner basis is easily computed, with no novel theoretical advances.

An algorithm to compute a Boolean Gröbner basis in a Boolean polynomial ring over an arbitrary coefficient Boolean ring was first introduced in (23). The key idea is a special monomial reduction which is more complicated than the usual monomial reduction in a polynomial ring over a field. While the algorithm has been implemented and is freely available (24; 26), the work is not well known to computer algebra researchers.

Recent work on Boolean Gröbner bases inspired us to return to them. Recent theoretical development can be found in (9; 11; 21), and has led to one of us developing an implementation of Boolean Gröbner bases (10) in the computer algebra system Risa/Asir (18).

In this paper, we survey our approach to Boolean Gröbner bases. In section 2, we review classical results of Boolean algebra in terms of Boolean rings. Section 3 is devoted to Boolean Gröbner bases, and section 4 considers comprehensive Boolean Gröbner bases. In section 5, we discuss an application to types of combinatorial problems like the popular puzzle Sudoku.

2. Boolean polynomial ring

In this section, we give several definitions and notations concerning Boolean polynomial rings, and then we show the *Boolean extension theorem* and *Boolean Nullstellensatz*, which are important classical results of Boolean algebra. We describe them in terms of Boolean polynomial rings. More details can be found in many text books of Boolean algebra, such as (20) for example.

Definition 1. A commutative ring $\mathbf{B}$ with an identity 1 is called *a Boolean ring* if every element a of $\mathbf{B}$ is idempotent, i.e. $a^2 = a$.

$(\mathbf{B},\vee,\wedge,\neg)$ becomes a Boolean algebra with the Boolean operations $\vee,\wedge,\neg$ defined by $a\vee b = a+b+a\cdot b, a\wedge b = a\cdot b, \neg a = 1+a$. Conversely, for a Boolean algebra $(\mathbf{B},\vee,\wedge,\neg)$, if we define $+$ and $\cdot$ by $a+b = (\neg a\wedge b)\vee(a\wedge\neg b)$ and $a\cdot b = a\wedge b$, $(\mathbf{B},+,\cdot)$ becomes a Boolean ring.
Since $-a = a$ in a Boolean ring, we do not need to use the symbol '$-$', however, we will use $-$ when we want to stress its meaning.
We use the symbol $\succeq$ to denote a partial order of a Boolean ring, that is $a \succeq b$ if and only if $ab = b$ for elements a, b of a Boolean ring $\mathbf{B}$.

Email addresses: ysato@rs.kagu.tus.ac.jp (Yosuke Sato), sinoue@rs.kagu.tus.ac.jp (Shutaro Inoue), sakira@kobe-u.ac.jp (Akira Suzuki), nabesima@ias.tokushima-u.ac.jp (Katsusuke Nabeshima), ksakai@math.tsukuba.ac.jp (Ko Sakai).

Example 1. Let S be an arbitrary set and $\mathcal{P}(S)$ be its power set, i.e. the family of all subsets of S. Then, $(\mathcal{P}(S), \vee, \wedge, \neg)$ becomes a Boolean algebra with the operations $\vee, \wedge, \neg$ as union, intersection and the complement of S respectively. As a Boolean ring, it is isomorphic to $\mathbb{GF}_2^S$ that is a commutative ring of all functions from S to $\mathbb{GF}_2$. Stone's representation theorem tells us any Boolean ring is isomorphic to a sub-algebra of $\mathbb{GF}_2^S$ for some set S. Especially, when $\mathbf{B}$ is a finite Boolean ring, it is isomorphic to a direct product $\mathbb{GF}_2^k$ for some natural number k. Note that a computable Boolean ring need not be finite. For any infinite set S, any family of computable subsets S which is closed under the computable operations $\vee, \wedge, \neg$ is a computable Boolean ring. For example a family of algebraically constructible subsets of K^l for some algebraically closed field K with a fixed natural number l forms a computable Boolean ring.

Definition 2. A non-zero element e of a Boolean ring $\mathbf{B}$ is said to be *atomic* if there does not exist a non-zero element c such that $ce = c$ except for $c = e$. *(*An atomic element is nothing but a non-zero minimal element w.r.t. $\succeq$. *)*

Lemma 3. *If* $\mathbf{B}$ *is a finite Boolean ring, it has at least one atomic element. Let* $e_1, \ldots, e_k$ *be all the atomic elements of* $\mathbf{B}$*, then* $e_i e_j = 0$ *for any* $i \neq j$ *and* $e_1 + \cdots + e_k = 1$*.*

proof We show the last equation, the rest is obvious. If $e_1 + \cdots + e_k \neq 1$, $e_1 + \cdots + e_k + 1 \neq 0$. Let c be a minimal element (an atomic element) of $\mathbf{B}$ such that $e_1 + \cdots + e_k + 1 \succeq c$, i.e. $c(e_1 + \cdots + e_k + 1) = c$. It follows that $c(e_1 + \cdots + e_k) = 0$. Since c is a minimal element, $c = e_i$ for some e_i, which leads us to a contradiction $e_i = e_i(e_1 + \cdots + e_k) = 0$. □

Definition 4. Let $\mathbf{B}$ be a Boolean ring. A quotient ring $\mathbf{B}[X_1, \ldots, X_n]/\langle X_1^2 - X_1, \ldots, X_n^2 - X_n\rangle$ with an ideal $\langle X_1^2 - X_1, \ldots, X_n^2 - X_n\rangle$ becomes a Boolean ring. It is called *a Boolean polynomial ring* and denoted by $\mathbf{B}(X_1, \ldots, X_n)$, its element is called *a Boolean polynomial*.

Note that a Boolean polynomial of $\mathbf{B}(X_1, \ldots, X_n)$ is uniquely represented by a polynomial of $\mathbf{B}[X_1, \ldots, X_n]$ that has at most degree 1 for each variable X_i. In what follows, we identify a Boolean polynomial with such a representation.

Multiple variables such as $X_1, \ldots, X_n$ or $Y_1, \ldots, Y_m$ are abbreviated to $\bar{X}$ or $\bar{Y}$ respectively. Lower small roman letters such as a, b, c are usually used for elements of a Boolean ring $\mathbf{B}$. The symbol $\bar{a}$ denotes an n-tuple of element of $\mathbf{B}$ for some n. For $\bar{a} = (a_1, \ldots, a_n)$ and $\bar{b} = (b_1, \ldots, b_m)$, $(\bar{a}, \bar{b})$ denotes an $(n+m)$-tuple $(a_1, \ldots, a_n, b_1, \ldots, b_m)$. For a Boolean polynomial $f(\bar{X}, \bar{Y})$ with variables $\bar{X}$ and $\bar{Y}$, $f(\bar{a}, \bar{Y})$ denote a Boolean polynomial in $\mathbf{B}(\bar{Y})$ obtained by specializing $\bar{X}$ with $\bar{a}$.

Definition 5. Let I be an ideal of $\mathbf{B}(X_1, \ldots, X_n)$. For a subset S of $\mathbf{B}$, $V_S(I)$ denotes a subset $\{\bar{a} \in S^n | \forall f \in I f(\bar{a}) = 0\}$. When $S = \mathbf{B}$, $V_{\mathbf{B}}(I)$ is simply denoted by $V(I)$ and called a *variety* of I. We say I is *satisfiable* in S if $V_S(I)$ is not empty. When $S = \mathbf{B}$, we simply say I is *satisfiable*.

Theorem 6 (Boolean extension theorem)**.** *Let* I *be a finitely generated ideal in a Boolean polynomial ring* $\mathbf{B}(Y_1, \ldots, Y_m, X_1, \ldots, X_n)$*.*
For any $\bar{b} \in V(I \cap \mathbf{B}(\bar{Y}))$*, there exist* $\bar{c} \in \mathbf{B}^n$ *such that* $(\bar{b}, \bar{c}) \in V(I)$*.*

proof It suffices to show the theorem for $n = 1$. Note first that any finitely generated ideal is principal in a Boolean ring, that is an ideal $\langle f_1, \ldots, f_s \rangle$ is equal to the principal ideal $\langle f_1 \vee \cdots \vee f_s \rangle$. Let $I = \langle fX_1 + g \rangle$ for some $f, g \in \mathbf{B}(\bar{Y})$. We claim that $I \cap \mathbf{B}(\bar{Y}) = \langle fg + g \rangle$. Since $(f+1)(fX_1 + g) = fg + g$, $fg + g \in I \cap \mathbf{B}(\bar{Y})$. Conversely, suppose that $h \in I \cap \mathbf{B}(\bar{Y})$, i.e. there exist $p, q \in \mathbf{B}(\bar{Y})$ such that $h = (pX_1 + q)(fX_1 + g)$. Then, $h = (pf + pg + qf)X_1 + qg$. Since $h \in \mathbf{B}(\bar{Y})$, we must have $pf + pg + qf = 0$, from which we have $h = qg = fqg + (f+1)qg = g(pf + pg) + (f+1)qg = gp(f+1) + (f+1)qg = (p+q)(f+1)g \in \langle fg + g \rangle$.
Suppose now that $\bar{b} \in V(\langle fg + g \rangle)$, that is $f(\bar{b})g(\bar{b}) + g(\bar{b}) = 0$. Let $c = (f(\bar{b}) + 1)d + g(\bar{b})$ where d can be any element of $\mathbf{B}$. Then $f(\bar{b})c + g(\bar{b}) = f(\bar{b})g(\bar{b}) + g(\bar{b}) = 0$. That is $(\bar{b}, c) \in V(I)$. □

Corollary 7 (Boolean weak Nullstellensatz)**.** *For any finitely generated ideal I of a Boolean polynomial ring $\mathbf{B}(X_1, \ldots, X_n)$, the variety $V(I) (\subseteq \mathbf{B}^n)$ of I is an empty set if and only if there exists a non-zero constant element of $\mathbf{B}$ in I.*

proof If $I \cap \mathbf{B} = \{0\}$, the above proof also works to show that $V(I) \neq \emptyset$. The converse is trivial. □

Theorem 8 (Boolean strong Nullstellensatz)**.** *Let I be a finitely generated ideal of a Boolean polynomial ring $\mathbf{B}(X_1, \ldots, X_n)$ such that $V(I) \neq \emptyset$.*
Then, for any Boolean polynomial $h(\bar{X}) \in \mathbf{B}(\bar{X})$,

$$h(\bar{X}) \in I \quad \text{if and only if} \quad \forall (\bar{b}) \in V(I)\ h(\bar{b}) = 0.$$

proof Let $I = \langle f(\bar{X}) \rangle$ and $\mathbf{B}'$ be a Boolean subring of $\mathbf{B}$ generated by all the coefficients of $f(\bar{X})$ and $h(\bar{X})$, i.e. $\mathbf{B}'$ is the smallest Boolean subring of $\mathbf{B}$ which includes all the coefficients of $f(\bar{X})$ and $h(\bar{X})$. First note that I is also satisfiable in $\mathbf{B}'$ by the Boolean weak Nullstellensatz. Secondly note that $\mathbf{B}'$ is finite, because each element of $\mathbf{B}'$ is a sum of finite elements which have a form $a_1^{n_1} a_2^{n_2} \cdots a_l^{n_l}$ where $a_1, a_2, \ldots, a_l$ are the coefficients of $f(\bar{X})$ and each n_i is either 0 or 1. By Lemma 3, $\mathbf{B}'$ has atomic elements $e_1, \ldots, e_k$ such that $e_i e_j = 0$ for any $i \neq j$ and $e_1 + \cdots + e_k = 1$. Suppose now that $\forall \bar{b} \in V(I)\ h(\bar{b}) = 0$. We certainly have the property:

$$\forall \bar{b} \in \mathbf{B}'^n (\ f(\bar{b}) = 0 \Rightarrow h(\bar{b}) = 0\ ) \qquad (1)$$

In order to show $h(\bar{X}) \in I$, we prove the following claims.

Claim 1: $f(b_1, \ldots, b_n) = 0 \Leftrightarrow e_i f(e_i b_1, \ldots, e_i b_n) = 0$ for each $i = 1, \ldots, k$.

proof of Claim1 We clearly have $f(b_1, \ldots, b_n) = 0 \Leftrightarrow e_i f(b_1, \ldots, b_n) = 0$ for each $i = 1, \ldots, k$.We also have the equation $e_i f(b_1, \ldots, b_n) = e_i f(e_i b_1, \ldots, e_i b_n)$.
The assertion follows from them. ⊠

Claim 2: $\forall (b_1, \ldots, b_n) \in \mathbf{B}'^n (\ e_i f(e_i b_1, \ldots, e_i b_n) = 0 \Rightarrow e_i h(e_i b_1, \ldots, e_i b_n) = 0\ )$ for each $i = 1, \ldots, k$.

proof of Claim2 Let i be fixed and suppose $e_i f(e_i b_1, \ldots, e_i b_n) = 0$ for elements $b_1, \ldots, b_n$ in $\mathbf{B}'$. Since I is satisfiable in $\mathbf{B}'$, we have elements $c_1, \ldots, c_n$ in $\mathbf{B}'$ such that $f(c_1, \ldots, c_n) = 0$. Let $a_j = e_i b_j + (1 + e_i) c_j$ for each $j = 1, \ldots, n$. Then, we have $e_i a_j = e_i b_j$ and $e_t a_j = e_t c_j$ for each $t \neq i$. By Claim 1, we have $f(a_1, \ldots, a_n) = 0$. By the property (1), we have $h(a_1, \ldots, a_n) = 0$. By Claim 1 again, we have $e_i h(e_i a_1, \ldots, e_i a_n) = 0$ which

is equivalent to $e_i h(e_i b_1, \ldots, e_i b_n) = 0$. ⊠

Claim 3: The ideal $\langle e_i f(\bar{X}), e_i(Uh(\bar{X}) + 1)\rangle \subseteq \mathbf{B}'(U, \bar{X})$ is unsatisfiable in $\mathbf{B}'$ for each $i = 1, \ldots, k$, where U is a new variable.

proof of Claim3 Assume that $e_i f(b_1, \ldots, b_n) = 0$ for some $(b_1, \ldots, b_n) \in \mathbf{B}'^n$. By Claim 1, we have $e_i f(e_i b_1, \ldots, e_i b_n) = 0$. By Claim 2, we have $e_i h(e_i b_1, \ldots, e_i b_n) = 0$. By Claim 1 again, we have $e_i h(b_1, \ldots, b_n) = 0$.
Therefore $e_i(Uh(b_1, \ldots, b_n) + 1) = e_i \neq 0$. ⊠

By the last claim and the Boolean weak Nullstellensatz, we can see the ideal $\langle e_i f(\bar{X}), e_i(Uh(\bar{X}) + 1)\rangle$ contains a non-zero element of $\mathbf{B}'$. Since e_i is an atomic element of $\mathbf{B}'$, it must contain e_i. So, there exist Boolean polynomials $p(U, \bar{X})$ and $q(U, \bar{X})$ of $\mathbf{B}'(U, \bar{X})$ such that $e_i = e_i f(\bar{X}) p(U, \bar{X}) + e_i(Uh(\bar{X}) + 1) q(U, \bar{X})$. Multiplying both sides by $h(\bar{X})$ and substituting 1 for U, we have $e_i h(\bar{X}) = e_i f(\bar{X}) p(1, \bar{X}) h(\bar{X})$, which shows that $e_i h(\bar{X}) \in I$. So, $h(\bar{X}) = e_1 h(\bar{X}) + \cdots + e_k h(\bar{X}) \in I$.
The converse is trivial. □

3. Boolean Gröbner bases

Boolean polynomial rings are essentially principal ideal rings, that is $\langle f_1, \ldots, f_l\rangle = \langle f_1 \vee \cdots \vee f_l\rangle$. Therefore it suffices to solve a single equation in order to solve a system of equations. A unary equation $aX = b$ for a variable X and elements a, b in a Boolean ring $\mathbf{B}$ has a solution if and only if $ab = b$. When there exists a solution, it has a form $X = b + (a + 1)P$ with a variable P which can have any value of $\mathbf{B}$. For a multivariate single equation $f(X_1, \ldots, X_n) = 0$, we can apply this process recursively to get a general form of a solution $X_1 = h_1(P1), X_2 = h_2(P_1, P_2), \ldots, X_n = h_n(P_1, P_2, \ldots, P_n)$ with parameters $P_1, P_2, \ldots, P_n$ which can have any value of $\mathbf{B}$. Therefore, it is very simple to solve a system of equations in a Boolean polynomial ring at least from a theoretical point of view. When the number l is not small, however, the size of a Boolean polynomial $\langle f_1 \vee \cdots \vee f_l\rangle$ exponentially increases with respect to l in general, and the above naive approach fails to apply for systems of equations of a Boolean polynomial ring.

The notion of Boolean Gröbner bases is one of the tools to overcome the above difficulty. A Boolean Gröbner basis is defined as a natural modification of a Gröbner basis in a polynomial ring over a field. Though it was introduced in (23) together with a computation algorithm using a special monomial reduction, the same notion was independently discovered by V.Weispfenning in a polynomial ring over a more general coefficient ring, namely, a commutative von Neumann regular ring (30). In this section, we describe Boolean Gröbner bases. For the proofs and more detailed descriptions, refer to (25) or (30).

In what follows, we assume that some admissible term order on a set of power products of variables is given. For a polynomial f in a polynomial ring $\mathbf{B}[\bar{X}]$ over a Boolean ring $\mathbf{B}$, we use the notations $LT(f)$, $LM(f)$ and $LC(f)$ to denote the leading power product, the leading monomial and leading coefficient of f respectively. $f - LM(f)$ is also denoted by $Rd(f)$. We also use the notations $LT(F)$ and $LM(F)$ to denote the sets $\{LT(f) | f \in F\}$ and $\{LM(f) | f \in F\}$ for a (possibly infinite) subset F of $\mathbf{B}[\bar{X}]$. $T(\bar{X})$ denotes the set of power products consisting of variables $\bar{X}$.

Definition 9. For an ideal I of a polynomial ring $\mathbf{B}[\bar{X}]$, a finite subset G of I is called a *Gröbner basis* of I if $\langle LM(I)\rangle = \langle LM(G)\rangle$.

Definition 10. For a polynomial $f \in \mathbf{B}[\bar{X}]$, let $a = LC(f)$, $t = LT(f)$ and $h = Rd(f)$. Let s is a term of $T(\bar{X})$, b is an element of $\mathbf{B}$ such that $ab \neq 0$ and p is any polynomial of $\mathbf{B}[\bar{X}]$. A *monomial reduction* $\rightarrow_f$ by f is defined as follows:

$$bts + p \rightarrow_f (1 - a)bts + absh + p.$$

*(*Note that $(bts + p) - ((1 - a)bts + absh + p) = bs(af)$.*)*
For a set $F \subseteq \mathbf{B}[\bar{X}]$, we write $g \rightarrow_F g'$ if and only if $g \rightarrow_f g'$ for some $f \in F$. A recursive closure of $\rightarrow_F$ is denoted by $\stackrel{*}{\rightarrow}_F$, i.e. $g \stackrel{*}{\rightarrow}_F g'$ if and only if $g = g'$ or there exist a sequence of monomial reductions $g \rightarrow_F g_1 \rightarrow_F \cdots \rightarrow_F g_n \rightarrow_F g'$.

Theorem 11. *When F is finite, $\rightarrow_F$ is noetherian, that is there is no infinite sequence of polynomials $g_1, g_2, \ldots$ such that $g_i \rightarrow_F g_{i+1}$ for each $i = 1, 2, \ldots$.*

Theorem 12. *Let I be an ideal of a polynomial ring $\mathbf{B}[\bar{X}]$.*
A finite subset G of I is a Gröbner basis of I if and only if $\forall h \in I$ $h \stackrel{*}{\rightarrow}_G 0$.

Using our monomial reductions, a reduced Gröbner basis is defined exactly as in a polynomial ring over a field. A Gröbner basis G is *reduced* if each polynomial of G is not reducible by a monomial reduction of any other polynomial of G. In a polynomial ring over a field, a reduced Gröbner basis is uniquely determined. In our case, however, this property does not hold.

Example 2. Let $\mathbf{B} = \mathbb{GF}_2 \times \mathbb{GF}_2$. In a polynomial ring $\mathbf{B}[X]$, $\{(1,0)X, (0,1)X\}$ and $\{(1,1)X\}$ are both reduced Gröbner bases of the same ideal.

In order to have a unique Gröbner basis, we need one more definition.

Definition 13. A reduced Gröbner basis G is said to be *stratified* if G does not contain two polynomials which have the same leading power product.

Theorem 14. *If G and G' are stratified Gröbner bases of the same ideal w.r.t. some term order, then $G = G'$.*

In the above example, $\{(1,1)X\}$ is the stratified Gröbner basis, but the other is not.

Definition 15. For a polynomial f, $LC(f)f$ is called a *Boolean closure* of f, and denoted by $bc(f)$. If $f = bc(f)$, f is said to be *Boolean closed*.

Theorem 16. *Let G be a Gröbner basis of an ideal I, then $bc(G) \setminus \{0\}$ is also a Gröbner basis of an ideal I.*

Theorem 17. *Let G be a reduced Gröbner basis, then every element is Boolean closed.*

S-polynomials are also defined similarly as in a polynomial ring over a field.

Definition 18. Let $f = atr + f'$ and $g = bsr + g'$ be polynomials where $a = LC(f)$, $b = LC(g)$, $tr = LT(f)$ and $sr = LT(g)$ for some power product t, s, r such that $GCD(t, s) = 1$, i.e. t and s do not contain a common variable. The polynomial $bsf + atg = bsf' + atg'$ is called an *S-polynomial* of f and g and denoted by $S(f, g)$.

As in a polynomial ring over a field, the following property is crucial for the construction of Gröbner bases.

Theorem 19. *Let G be a finite set of polynomials such that each element of G is Boolean closed. Then, G is a Gröbner basis if and only if $S(f,g) \xrightarrow{*}_G 0$ for any pair f, g of G.*

For any given finite set F, using our monomial reductions, we can always construct a Gröbner basis of $\langle F \rangle$ by computing Boolean closures and S-polynomials with the following algorithms. It is also easy to construct a stratified Gröbner basis from a Gröbner basis.

Algorithm `BC`
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: F' a set of Boolean closed polynomials such that $\langle F' \rangle = \langle F \rangle$
`begin`
$F' = \emptyset$
`while there exists a polynomial` $f \in F$ `which is not Boolean closed`
$F = F \cup \{bc(f) - f\} \setminus \{f\}$, $F' = F' \cup \{bc(f)\}$
`end.`

Algorithm `GBasis`
Input: F a finite subset of $\mathbf{B}[\bar{X}]$, $>$ a term order of $T(\bar{X})$
Output: G a Gröbner basis of $\langle F \rangle$ w.r.t. $>$
`begin`
G `= BC(`F`)`
`while there exists two polynomials` $p, q \in G$ `such that` $S(p,q) \xrightarrow{*}_G h$
`for some non-zero polynomial` h `which is irreducible by` $\rightarrow_G$
G `= `$G \cup$`BC(`$\{h\}$`)`
`end.`

Since any element of a Boolean ring is idempotent, a Boolean polynomial ring is more natural to work on. We can also define Gröbner bases in Boolean polynomial rings. A power product $X_1^{l_1} \cdots X_n^{l_n}$ is called a *Boolean power product* if each l_i is either 0 or 1. The set of all Boolean power products consisting of variables $\bar{X}$ is denoted by $BT(\bar{X})$. A Boolean polynomial $f(\bar{X})$ in $\mathbf{B}(\bar{X})$ is uniquely represented by $b_1 t_1 + \cdots + b_k t_k$ with elements $b_1, \ldots, b_k$ of $\mathbf{B}$ and distinct Boolean power products $t_1, \ldots, t_k$. We call $b_1 t_1 + \cdots + b_k t_k$ the *canonical representation* of $f(\bar{X})$. Since $BT(\bar{X})$ is a subset of $T(\bar{X})$, a term order $\geq$ on $T(\bar{X})$ is also defined on $BT(\bar{X})$. Given such a term order $\geq$, we use the same notations $LT(f), LM(f), LC(f)$ and $Rd(f)$ as before, which are defined by using its canonical representation. We also use the same notations $LT(F)$ and $LM(F)$ for a set F of Boolean polynomials as before.

Definition 20. For an ideal I of a Boolean polynomial ring $\mathbf{B}(\bar{X})$, a finite subset G of I is called a *Boolean Gröbner basis* of I if $\langle LM(I) \rangle = \langle LM(G) \rangle$ in $\mathbf{B}(\bar{X})$.

Using canonical representations of Boolean polynomials, we can also define monomial reductions for Boolean polynomials as Definition 10 and have the same property of Theorem 11 and 12. We can also define a stratified Boolean Gröbner basis as in Definition 13, which is unique w.r.t. a term order. The Boolean closure of a Boolean polynomial is also

similarly defined as Definition 15 and the same properties of Theorem 14,16 and 17 hold. Construction of a Boolean Gröbner basis is very simple. Given a finite set of Boolean polynomials $F \subseteq \mathbf{B}(\bar{X})$. Compute a Gröbner basis G of the ideal $\langle F \cup \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}\rangle$ in $\mathbf{B}[\bar{X}]$ w.r.t. the same term order. Then, $G \setminus \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$ is a Boolean Gröbner basis of $\langle F\rangle$ in $\mathbf{B}(\bar{X})$. If G is stratified, then $G \setminus \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$ is also stratified.

Example 3. The following left constraints with unknown set variables X and Y and an unknown element variable a is equivalent to the right system of equations of a Boolean polynomial ring $\mathbf{B}(X, Y, A)$, where $\mathbf{B}$ is a Boolean ring of sets and the variable A stands for the singleton $\{a\}$.

$$\begin{cases} X \cup Y \subseteq \{1,2\} \\ 1 \in X \\ a \in Y \\ X \cap Y = \emptyset \end{cases} \iff \begin{cases} (XY + X + Y) + \{1,2\}(XY + X + Y) = 0 \\ \{1\}X + \{1\} = 0 \\ AY + A = 0 \\ XY = 0 \end{cases}$$

The stratified Boolean Gröbner basis G of the ideal
$I = \langle (XY + X + Y) + \{1,2\}(XY + X + Y), \{1\}X + \{1\}, AY + A, XY\rangle$
w.r.t. a lexicographic term order $X > Y > A$ has the following form:
$G = \{\{2\}XY, \{2\}YA + \{2\}A, (1 + \{2\})Y, \{2\}XA, (1 + \{2\})X + \{1\}, (1 + \{2\})A\}$. From this we can get the elimination ideal $I \cap \mathbf{B}(A) = \langle (1 + \{2\})A\rangle$. By the Boolean extension theorem, we can see that the given constraint is satisfiable if and only if the element variable a satisfies the equation $(1 + \{2\})\{a\} = 0$ that is $a = 2$.

We conclude this section with the following theorem, which is essentially a special instance of Theorem 2.3 of (30).

Definition 21. Let $\mathbf{B}$ be a Boolean ring and k be a natural number. $\mathbf{B}^k$ denotes a direct product, i.e. the set of all k-tuples of elements of $\mathbf{B}$. For an element p of $\mathbf{B}^k$, $p_i \in \mathbf{B}$ denotes the i-th element of p for each $i = 1, \ldots, k$. If we define $p + q$ and $p \cdot q$ for $p, q \in \mathbf{B}^k$ by $(p + q)_i = p_i + q_i$ and $(p \cdot q)_i = p_i \cdot q_i$ for each $i = 1, \ldots, k$, $\mathbf{B}^k$ also becomes a Boolean ring. For a polynomial $f(\bar{X})$ in $\mathbf{B}^k[\bar{X}]$ $f_i (i = 1, \ldots, k)$ denotes the polynomial in $\mathbf{B}[\bar{X}]$ obtained by replacing each coefficient p of f by p_i. For a Boolean polynomial $f(\bar{X})$ in $\mathbf{B}^k(\bar{X})$, a Boolean polynomial f_i in $\mathbf{B}(\bar{X})$ is defined similarly.

Theorem 22. *In a polynomial ring $\mathbf{B}^k[\bar{X}]$, let G be a finite set of Boolean closed polynomials. Then, G is a (reduced) Gröbner basis of an ideal I if and only if $G_i = \{g_i | g \in G\} \setminus \{0\}$ is a (reduced) Gröbner basis of the ideal $I_i = \{f_i | f \in I\}$ in $\mathbf{B}[\bar{X}]$ for each $i = 1, \ldots, k$.*

Corollary 23. *In a Boolean polynomial ring $\mathbf{B}^k(\bar{X})$, let G be a finite set of Boolean closed Boolean polynomials. Then, G is a (reduced) Boolean Gröbner basis of an ideal I if and only if $G_i = \{g_i | g \in G\} \setminus \{0\}$ is a (reduced) Gröbner basis of the ideal $I_i = \{f_i | f \in I\}$ in $\mathbf{B}(\bar{X})$ for each $i = 1, \ldots, k$.*

4. Comprehensive boolean Gröbner bases

In a polynomial ring over a field, construction of a comprehensive Gröbner basis is not so simple in general. In order to get a uniform (with respect to parameters) representation of reduced Gröbner bases, we need to divide a parameter space into several partitions according to the conditions that parameters satisfy. (See (13; 16; 17; 28; 29; 31).) The most crucial reason is that a polynomial ring over a field is not a field itself.

In our case, however, a Boolean polynomial ring is also a Boolean ring. This obvious fact enables us to easily construct a stratified comprehensive Boolean Gröbner basis. We do not even need to divide a parameter space.

In this section, we first present a naive method to construct comprehensive Boolean Gröbner bases, then we show an alternative method based on our recent result (9), which is much faster than the first naive method in most cases.

4.1. Naive method

In what follows, we use variables $\bar{A} = A_1, \ldots, A_m$ for parameters and variables $\bar{X} = X_1, \ldots, X_n$ for main variables. We also assume that some admissible term order on $T(\bar{X})$ is given.

Definition 24. Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ be a finite subset of a Boolean polynomial ring $\mathbf{B}(\bar{A}, \bar{X})$. A finite subset $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_k(\bar{A}, \bar{X})\}$ of $\mathbf{B}(\bar{A}, \bar{X})$ is called a *comprehensive Boolean Gröbner basis* of F, if $G(\bar{a}) = \{g_1(\bar{a}, \bar{X}), \ldots, g_k(\bar{a}, \bar{X})\} \setminus \{0\}$ is a Boolean Gröbner basis of the ideal $\langle F(\bar{a})\rangle = \langle f_1(\bar{a}, \bar{X}), \ldots, f_l(\bar{a}, \bar{X})\rangle$ in $\mathbf{B}'(\bar{X})$ for any Boolean extension $\mathbf{B}'$ of $\mathbf{B}$, i.e. a Boolean ring which includes $\mathbf{B}$ as a subring, and any $\bar{a} = (a_1, \ldots, a_m) \in \mathbf{B}'^m$. G is also said to be *stratified* if $G(\bar{a})$ is stratified for any $\bar{a} = (a_1, \ldots, a_m) \in \mathbf{B}'^m$.

Theorem 25. *Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ be a finite subset of a Boolean polynomial ring $\mathbf{B}(\bar{A}, \bar{X})$. Considering $\mathbf{B}(\bar{A}, \bar{X})$ as a Boolean polynomial ring $(\mathbf{B}(\bar{A}))(\bar{X})$ with the coefficient Boolean ring $\mathbf{B}(\bar{A})$, let $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_k(\bar{A}, \bar{X})\}$ be a (stratified) Boolean Gröbner basis of the ideal $\langle F\rangle$ in this polynomial ring. Then G becomes a (stratified) comprehensive Boolean Gröbner basis of F.*

proof Let $\mathbf{B}'$ be a Boolean extension of $\mathbf{B}$. Note first that G is also a (stratified) Boolean Gröbner basis of $\langle F\rangle$ in $(\mathbf{B}'(\bar{A}))(\bar{X})$. Therefore, it suffices to consider only specialization from $\mathbf{B}$. Let $\bar{a} = a_1, \ldots, a_m$ be an arbitrary m-tuple of elements of $\mathbf{B}$. Note that the specialization of parameters $\bar{A}$ with $\bar{a}$ induces a homomorphism from $\mathbf{B}(\bar{A}, \bar{X})$ to $\mathbf{B}(\bar{X})$. We clearly have $\langle F(\bar{a})\rangle = \langle G(\bar{a})\rangle$ in $\mathbf{B}(\bar{X})$. If $f(\bar{A}, \bar{X}) \rightarrow_{g(\bar{A},\bar{X})} h(\bar{A}, \bar{X})$ in $(\mathbf{B}(\bar{A}))(\bar{X})$, then $f(\bar{A}, \bar{X}) = p(\bar{A})ts + f'(\bar{A}, \bar{X})$, $g(\bar{A}, \bar{X}) = q(\bar{A})t + g'(\bar{A}, \bar{X})$ and $h(\bar{A}, \bar{X}) = (1 - q(\bar{A}))p(\bar{A})ts + q(\bar{A})p(\bar{A})sg'(\bar{A}, \bar{X}) + f'(\bar{A}, \bar{X})$ for some $t, s \in T(\bar{X})$ and $p(\bar{A}), q(\bar{A}) \in \mathbf{B}(\bar{A})$ and $f'(\bar{A}, \bar{X})$, $g'(\bar{A}, \bar{X}) \in \mathbf{B}(\bar{A}, \bar{X})$, where $q(\bar{A})t$ is the Boolean leading monomial of $g(\bar{A}, \bar{X})$. In case $q(\bar{a})p(\bar{a}) \neq 0$, certainly $q(\bar{a}) \neq 0$ and $p(\bar{a}) \neq 0$, so $q(\bar{a})t$ is the Boolean leading monomial of $g(\bar{a}, \bar{X})$ and $p(\bar{a})ts$ is a monomial of $f(\bar{A}, \bar{X})$ and $f(\bar{a}, \bar{X}) \rightarrow_{g(\bar{a},\bar{X})} h(\bar{a}, \bar{X})$. Otherwise, $h(\bar{a}, \bar{X}) = f(\bar{a}, \bar{X})$. In either case, we have $f(\bar{a}, \bar{X}) \overset{*}{\rightarrow}_{g(\bar{a},\bar{X})} h(\bar{a}, \bar{X})$. Therefore, if $f(\bar{A}, \bar{X}) \rightarrow_G h(\bar{A}, \bar{X})$ in $(\mathbf{B}(\bar{A}))(\bar{X})$, then we have $f(\bar{a}, \bar{X}) \overset{*}{\rightarrow}_{G(\bar{a})} h(\bar{a}, \bar{X})$ in $\mathbf{B}(\bar{X})$. Any Boolean polynomial in the ideal $\langle F(\bar{a})\rangle$ is equal to $f(\bar{a}, \bar{X})$ for some Boolean polynomial $f(\bar{A}, \bar{X})$ in the ideal $\langle F\rangle$ of $(\mathbf{B}(\bar{A}))(\bar{X})$. Since G is

a Boolean Gröbner basis of $\langle F\rangle$, we have $f(\bar{A},\bar{X}) \xrightarrow{*}_G 0$. By the above observation, we have $f(\bar{a},\bar{X}) \xrightarrow{*}_{G(\bar{a})} 0$. This shows that G is a comprehensive Boolean Gröbner basis of F.
Suppose G is stratified, then any element g of G is Boolean closed.
So, if $LC(g)(\bar{a}) = 0$, then $g(\bar{a},\bar{X})$ must be equal to 0. Therefore, unless $g(\bar{a},\bar{X}) = 0$, we have $LT(g(\bar{a},\bar{X})) = LT(g(\bar{A},\bar{X}))$. Now it is clear that $G(\bar{a})$ is stratified. □

Example 4. For the same ideal of Example 3, the stratified Boolean Gröbner basis of I in the Boolean polynomial ring $(\mathbf{B}(A))(X,Y)$ has the following form:

$$\{(\{2\}A+\{2\})XY, (1+A+\{2\})X+\{1\}A+\{1\}, (1+A+\{2\})Y+\{2\}A, (1+\{2\})A\}.$$

From this, we can get the elimination ideal $I\cap\mathbf{B}(A) = \langle(1+\{2\})A\rangle$. Moreover, if we specialize the variable A with $\{2\}$, it becomes the stratified Boolean Gröbner basis $\{X+\{1\}, Y+\{2\}\}$.

4.2. Alternative method

Let F be a finite set of $\mathbf{B}(\bar{A},\bar{X})$. As is described in the previous subsection, a (stratified) Boolean Gröbner basis G computed in the Boolean polynomial ring $(\mathbf{B}(\bar{A}))(\bar{X})$ becomes a (stratified) comprehensive Boolean Gröbner basis of F. When the $\bar{X}$-eliminate portion $\langle F\rangle\cap\mathbf{B}(\bar{A})$ is not a trivial ideal $\{0\}$, however, the size of G tends to be extremely big. In such a case, the computation often does not terminate within a practical time. In order to overcome this difficulty, a block term order is useful. We will show that a Boolean Gröbner basis computed with a block term order such that $\bar{X} \gg \bar{A}$ becomes a comprehensive Boolean Gröbner basis of F. In order to prove this fact, we need the following well-known fact which is easy in itself.

Lemma 26. *Let $R[\bar{A},\bar{X}]$ be a polynomial ring with variables $\bar{A}$ and $\bar{X}$ over a commutative ring R with an identity. Let I be an ideal of this polynomial ring. Let $>$ be a block term order of $T(\bar{A},\bar{X})$ such that $\bar{X} \gg \bar{A}$ and G be a Gröbner basis of I w.r.t. $>$. Then G is also a Gröbner basis of I w.r.t. $>_{\bar{X}}$ regarding $R[\bar{A},\bar{X}]$ as a polynomial ring over the coefficient ring $R[\bar{A}]$, that is $\langle\{LM(g)|g\in G\}\rangle = \langle\{LM(f)|f\in I\}\rangle$. Where $>_{\bar{X}}$ denotes a restriction of $>$ to $T(\bar{X})$.*

In the lemma, obviously we can replace R by a Boolean ring $\mathbf{B}$, furthermore the lemma also holds if we replace $R[\bar{A},\bar{X}]$ and $R[\bar{A}]$ by $\mathbf{B}(\bar{A},\bar{X})$ and $\mathbf{B}(\bar{A})$ respectively. By this observation together with Theorem 25, the following theorem directly follows.

Theorem 27. *Let $G = \{g_1(\bar{A},\bar{X}),\ldots,g_k(\bar{A},\bar{X})\}$ be a Boolean Gröbner basis of $F = \{f_1(\bar{A},\bar{X}),\ldots,f_l(\bar{A},\bar{X})\}$ in a Boolean polynomial ring $\mathbf{B}(\bar{A},\bar{X})$ w.r.t. a block term order $>$ such that $\bar{X} \gg \bar{A}$. Then G is a comprehensive Boolean Gröbner basis of F w.r.t. $>_{\bar{X}}$.*

In the above theorem, $G = \{g_1(\bar{a},\bar{X}),\ldots,g_k(\bar{a},\bar{X})\}$ may not be stratified or reduced even if $G = \{g_1(\bar{A},\bar{X}),\ldots,g_k(\bar{A},\bar{X})\}$ is stratified, because G may not be reduced as a Boolean Gröbner basis in $(\mathbf{B}(\bar{A}))(\bar{X})$.

Example 5. In Example 3, the stratified Boolean Gröbner basis G of the ideal
$I = \langle(XY+X+Y)+\{1,2\}(XY+X+Y), \{1\}X+\{1\}, AY+A, XY\rangle$
w.r.t. a lexicographic term order $X > Y > A$ has the following form:

$G = \{\{2\}XY, \{2\}YA + \{2\}A, (1 + \{2\})Y, \{2\}XA, (1 + \{2\})X + \{1\}, (1 + \{2\})A\}$.
By the above theorem, G is a comprehensive Boolean Gröbner basis of $\{(XY + X + Y) + \{1, 2\}(XY + X + Y), \{1\}X + \{1\}, AY + A, XY\}$ with main variables X, Y and a parameter A w.r.t. a lexicographic term order $X > Y$. If we specialize A with $\{2\}$, G becomes $\{\{2\}XY, \{2\}Y + \{2\}, (1 + \{2\})Y, \{2\}X, (1 + \{2\})X + \{1\}, 0\}$. Obviously it is not even reduced.

Let us conclude this section with the following obvious but important fact, which actually plays an important role in the application of Boolean Gröbner bases described in the next section.

Corollary 28. *Let $G = \{g_1(\bar{X}), \ldots, g_k(\bar{X})\}$ be a Boolean Gröbner basis of $F = \{f_1(\bar{X}), \ldots, f_l(\bar{X})\}$ in a Boolean polynomial ring $\mathbf{B}(\bar{X})\}$ w.r.t. a purely lexicographic term order such that $X_n > X_{n-1} > \cdots > X_1$. Then G is a comprehensive Boolean Gröbner basis of F regarding $X_i, \ldots, X_1$ as parameters, for each $i = 1, \ldots, n - 1$.*

5. Applications

We discuss applications of Boolean Gröbner bases in this section. We first observe the following fact.

Theorem 29. *Let $F = \{f_1(\bar{X}), \ldots, f_l(\bar{X})\}$ be a finite set of Boolean polynomials in $\mathbf{B}(\bar{X})$ such that $\langle F\rangle$ is satisfiable, and $G = \{g_1(\bar{X}), \ldots, g_t(\bar{X})\}$ be the stratified Boolean Gröbner basis of $\langle F\rangle$ w.r.t. a purely lexicographic term order such that $X_n > X_{n-1} > \cdots > X_1$. For each $i = 1, \ldots, n - 1$, let G^i denote $G \cap \mathbf{B}(X_1, \ldots, X_i)$. For any i-tuple $(c_1, \ldots, c_i)$ of elements in $\mathbf{B}$ such that $(c_1, \ldots, c_i) \in V(\langle G^i\rangle)$, let $a_1X_{i+1} + b_1, \ldots, a_kX_{i+1} + b_k$ be all the unary polynomials of the variable X_{i+1} which apper in $\{g_1(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n), \ldots, g_t(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n)\}$. Then, $\{a_1X_{i+1} + b_1, \ldots, a_kX_{i+1} + b_k\}$ is a Boolean Gröbner basis of $\langle f_1(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n), \ldots, f_l(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n)\rangle \cap \mathbf{B}(X_{i+1})$. Furthermore $\{(a_1 \vee \cdots \vee a_k)X_{i+1} + (b_1 \vee \cdots \vee b_k)\}$ is a stratified Boolean Gröbner basis of the same ideal.*

proof The first assertion is a direct consequence of Corollary 28 and a basic property of Gröbner bases. We show the second assertion. Note first that each polynomial in $\{a_1X_{i+1} + b_1, \ldots, a_kX_{i+1} + b_k\}$ is Boolean closed. Suppose otherwise, we have a non-zero constant in the ideal $\langle f_1(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n), \ldots, f_l(c_1, \ldots, c_i, X_{i+1}, \ldots, X_n)\rangle$ of $\mathbf{B}(X_{i+1}, \ldots, X_n)$. Hence, the ideal is unstisfiable by the Boolean weak Nullstellensatz, which contradicts the Boolean extension theorem. Similarly an S-polynomial of any pair of $\{a_1X_{i+1} + b_1, \ldots, a_kX_{i+1} + b_k\}$ is equal to 0. Summarizing the above, we have $a_jb_j = b_j$ and $a_jb_{j'} = a_{j'}b_j$ for each distict j and j'. With these equations, we can easily check that $\langle a_1X_{i+1} + b_1, \ldots, a_kX_{i+1} + b_k\rangle = \langle (a_1 \vee \cdots \vee a_k)X_{i+1} + (b_1 \vee \cdots \vee b_k)\rangle$. Since $(a_1 \vee \cdots \vee a_k)X_{i+1} + (b_1 \vee \cdots \vee b_k)$ is a Boolean closed polynomial, it is a Boolean Gröbner basis. □

For a given system of equations of a Boolean polynomial ring, once we have a staratified Boolean Gröbner basis w.r.t. a purely lexicographic term order, we can easily construct a specific solution by the above theorem. This method is also applicable when we are not interested in all solutions but only in some restricted solutions. We conlude the section with such an example.

A Sudoku puzzle can be considered as a system of equations of a certain Boolean polynomial ring. Though the most popular Sudoku puzzles are 9×9, we consider the following 4×4 Sudoku puzzle in order to make it easy to understand.

1			
		3	
	2		

We associate a variable X_{ij} for each grid at the i-th row and the j-th column. This puzzle can be considered as a set constraint where each variable should be assigned a singleton set from 4 candidates $\{1\}, \{2\}, \{3\}, \{4\}$ so that any distinct two variables which lie on a same row, column or block must be assigned different singleton sets. 3 variables are assigned singleton sets $X_{11} = \{1\}, X_{23} = \{3\}, X_{32} = \{2\}$ as the initial conditions. This constraint is translated into a system of equations of a Boolean polynomial ring $\mathbf{B}(X_{11}, X_{12}, \ldots, X_{44})$ with $\mathbf{B} = \mathcal{P}(\{1, 2, 3, 4\})$ as follows:

(1) $X_{11} = \{1\}, X_{23} = \{3\}, X_{32} = \{2\}$.
(2) $X_{ij}X_{i'j'} = 0 (= \emptyset)$ for each pair of distinct variables $X_{ij}, X_{i'j'}$ which lie on a same row, column or block.
(3) $\sum_{(i,j)\in A} X_{ij} = 1 (= \{1, 2, 3, 4\})$ where A is a set of indices lying on a same row, column or block. (There are 12 such A's.)

This puzzle is nothing but solving the above equations with a strong restriction that is each variable must be a singleton set. Unless we have this restriction, we can solve the equations by computing a stratified boolean Gröbner basis of the corresponding ideal as described above. The stratified Boolean Gröbner basis G w.r.t. a purely lexicographic term order such that $X_{44} > X_{43} > \cdots > X_{12} > X_{11}$ has the following form: $G = \{X_{44} + \{2\}X_{13}, X_{43} + \{4\}X_{31} + \{2\}X_{13} + \{2\}, X_{42} + \{4\}X_{21} + \{1\}, X_{41} + \{4\}X_{31} + \{4\}X_{21} + \{3, 4\}, X_{34} + \{4\}X_{13} + \{3\}, X_{33} + \{4\}X_{31} + \{4\}X_{13} + \{1, 4\}, X_{32} + \{2\}, \{4\}X_{31}X_{21}, \{4\}X_{31}X_{13}, (1+\{4\})X_{31}, X_{24}+\{4\}X_{12}+\{1\}, X_{23}+\{3\}, X_{22}+\{4\}X_{21}+\{4\}X_{12}+\{4\}, \{4\}X_{21}X_{12}, (1+\{4\})X_{21}+\{2\}, X_{14}+\{2, 4\}X_{13}+\{4\}X_{12}+\{2, 4\}, \{4\}X_{13}X_{12}, (1 + \{2, 4\})X_{13}, (1 + \{4\})X_{12} + \{3\}, X_{11} + \{1\}\}$.

Though this Gröbner basis is not yet a solution of the constraint, it can be considered as a kind of *compiled form* of the Sudoku puzzle. That is, we do not need to know any rule of Sudoku puzzles, we can simply solve a unary equations step by step from the lowest variable to the highest variable in order to get a solution. In this example, X_{11} already has a specific value $\{1\}$, the only singleton solution of the equation $(1+\{4\})X_{12}+\{3\} = 0$ is $X_{12} = \{3\}$. Specializing X_{11} with $\{1\}$ and X_{12} with $\{3\}$, G becomes $\{X_{44}+\{2\}X_{13}, X_{43}+\{4\}X_{31} + \{2\}X_{13} + \{2\}, X_{42} + \{4\}X_{21} + \{1\}, X_{41} + \{4\}X_{31} + \{4\}X_{21} + \{3, 4\}, X_{34} + \{4\}X_{13} + \{3\}, X_{33} + \{4\}X_{31} + \{4\}X_{13} + \{1, 4\}, X_{32} + \{2\}, \{4\}X_{31}X_{21}, \{4\}X_{31}X_{13}, (1 + \{4\})X_{31}, X_{24}+\{1\}, X_{23}+\{3\}, X_{22}+\{4\}X_{21}+\{4\}, (1+\{4\})X_{21}+\{2\}, X_{14}+\{2, 4\}X_{13}+\{2, 4\}, (1 + \{2, 4\})X_{13}\}$. The equation $(1 + \{2, 4\})X_{13} = 0$ has two singleton solutions $X_{13} = \{2\}$ and $X_{13} = \{4\}$. If we specialize X_{13} with $\{4\}$, G becomes $\{X_{44}, X_{43} + \{4\}X_{31}+\{2\}, X_{42}+\{4\}X_{21}+\{1\}, X_{41}+\{4\}X_{31}+\{4\}X_{21}+\{3, 4\}, X_{34}+\{4\}+\{3\}, X_{33}+\{4\}X_{31} + \{1\}, X_{32} + \{2\}, \{4\}X_{31}X_{21}, \{4\}X_{31}, (1 + \{4\})X_{31}, X_{24} + \{1\}, X_{23} + \{3\}, X_{22} +$

$\{4\}X_{21} + \{4\}, (1 + \{4\})X_{21} + \{2\}, X_{14} + \{2\}\}$. Obviously it has no singleton solutions since $X_{44} = 0$. On the other hand, specializing X_{13} with $\{2\}$, G becomes $\{X_{44} + \{2\}, X_{43} + \{4\}X_{31}, X_{42} + \{4\}X_{21} + \{1\}, X_{41} + \{4\}X_{31} + \{4\}X_{21} + \{3, 4\}, X_{34} + \{3\}, X_{33} + \{4\}X_{31} + \{1, 4\}, X_{32} + \{2\}, \{4\}X_{31}X_{21}, (1 + \{4\})X_{31}, X_{24} + \{1\}, X_{23} + \{3\}, X_{22} + \{4\}X_{21} + \{4\}, (1 + \{4\})X_{21} + \{2\}, X_{14} + \{4\}\}$. X_{14} has a specific value $\{4\}$ and X_{21} has the only singleton solution $\{2\}$. Specializing X_{14} with $\{4\}$ and X_{21} with $\{2\}$, G becomes $X_{44} + \{2\}, X_{43} + \{4\}X_{31}, X_{42} + \{1\}, X_{41} + \{4\}X_{31} + \{3, 4\}, X_{34} + \{3\}, X_{33} + \{4\}X_{31} + \{1, 4\}, X_{32} + \{2\}, (1 + \{4\})X_{31}, X_{24} + \{1\}, X_{23} + \{3\}, X_{22} + \{4\}\}$. Now we have specific solutions $X_{22} = \{4\}$,$X_{23} = \{3\}$ and $X_{24} = \{1\}$. The equation $(1 + \{4\})X_{31} = 0$ has the only singleton solution $X_{31} = \{4\}$. Specializing those values we finally get a solution $X_{44} = \{2\}, X_{43} = \{4\}, X_{42} = \{1\}, X_{41} = \{3\}, X_{34} = \{3\}, X_{33} = \{1\}, X_{32} = \{2\}, X_{24} = \{1\}, X_{23} = \{3\}, X_{22} = \{4\}, X_{14} = \{4\}, X_{11} = \{1\}$.

The above method is not only for solving Sudoku puzzles, it can handle any set constraint with additional restrictions such as singleton set solutions or non-empty set solutions. The above naive method is also sufficiently practical for 9×9 Sudoku puzzles. We can solve most Sudoku puzzles including variants such as diagonal Sudoku by the same program we implemented.

The 4×4 Sudoku puzzles are called *Shidoku* puzzles. In (1), a naive method to solve a Shidoku puzzle by computation of a Boolean Gröbner basis of a Boolean polynomial ring over the simplest coefficient Boolean ring $\mathbb{GF}_2$ is discussed, where we have to use $4^3 = 64$ variables. The method gives a canonical representation of the solutions of a given Shidoku puzzle. When there exists a unique solution, the computed Boolean Gröbner basis corresponds to it. The method is complete at least from a theoretical point of view. It does not need any pruned tree search as discussed above. However, for solving 9×9 Sudoku puzzles we have to use $9^3 = 729$ variables, and the computations of Boolean Gröbner bases (or any other method to solve such Boolean equations) become extremely heavy.

In (11), more sophisticated techniques are proposed. We can solve set constraints with restrictions as described above by only computations of Boolean Gröbner bases w.r.t. any term order. We do not need any technique to optimize the tree search such as discussed in (2). They are implemented in the computer algebra system Risa/Asir and released as a free software in (10).

6. Conclusion and Remarks

The origins of studies of Boolean Gröbner bases go back to the old works of (12) and (22). They also deal with only Boolean polynomial rings over $\mathbb{GF}_2$. The first paper of Boolean Gröbner bases which discusses a general Boolean ring as a coefficient ring is (23). The similar notion of monomial reductions of Boolean polynomials was independently discovered by (30) in a different situation, namely in a polynomial ring over a commutative von Neumann regular ring. These works led us to the discovery of the closed relationship between Boolean Gröbner bases and comprehensive Gröbner bases.

Other methods to solve Sudoku puzzles using Gröbner bases are also studied in several papers such as (1; 4; 7), however our approach with general Boolean Gröbner bases has brought us the first ever practical Sudoku solver by computations of Gröbner bases.

References

[1] Arnold,E., Lucas,S.K. and Taalman,L.(2010). Gröbner Basis representations of Sudoku. College Math. J. 41(2) pp 101-111.

[2] Bernasconi, A., Codenotti, B., Crespi, V. and Resta, G.(1997). Computing Gröbner bases in the Boolean setting with applications to counting. In Proceedings of the Workshop on Algorithm Engineering (WAE 97), G. Italiano & S. Orlando, eds., University of Venice, Venice, September 11-13, 1997, pp 209–218.

[3] Brickenstein,M., Dreyer, A., Greuel, G.-M., Wedler, M. and Wienand,O. (2009). New developments in the theory of Groebner bases and applications to formal verification. Journal of Pure and Applied Algebra, Vol. 213 pp 1612-1635.

[4] Falcon,R.M. and Martin-Morales,J.(2007). Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7. J. Symb. Comp. 42/11-12, pp 1142–1154.

[5] Faugere, J.-C., Joux, A. (2003). Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner bases. In Proceedings of CRYPTO 2003 Boneh, D. (ed.) Springer LNCS 2729, pp 4460

[6] Faugere, J.-C. (2003). Solving Structured Polynomial Systems and Applications to Cryptology. In Proceedings of CASC 2009, Springer LNCS 5743, pp 79-80.

[7] Gago-Vargas, J. et al. (2006). Sudokus and Gröbner Bases: Not Only a *Divertimento*. In Proceedings of CASC 2006, pp 155-165, Springer LNCS 4194, 2006.

[8] Gerdt, V.P.; Zinin, M.V.(2008). A Pommaret division algorithm for computing Gröbner bases in Boolean rings. In Proceedings of ISSAC 2008, pp 95–102.

[9] Inoue, S. (2009). On the computations of Boolean Gröbner bases. In Proceedings of CASC 2009, Springer LNCS 5743, pp 130-141.

[10] Inoue, S. (2009). BGSet - Boolean Groebner bases for Sets -.
`http://www.mi.kagu.tus.ac.jp/~inoue/BGSet/`

[11] Inoue, S. and Sato, Y.(2010). Computation of minimal polynomials in Boolean Polynomial rings. Submitted for publication.

[12] Kandri-Rody,A., Kapur,D. and Narendran,P. (1985). An Ideal-Theoretic Approach for Word Problems and Unification Problems over Commutative Algebras. In Proceedings *First International Conference on Rewriting Techniques and Applications (RTA-85)*, Dijon, France (eds. Jouannaud and Musser), pp 345–364. Springer LNCS 202.

[13] Kapur, D. (1995). An Approach for Solving Systems of Parametric Polynomial Equations. in *Principles and Practices of Constraint Programming.* (eds. Saraswat and Van Hentenryck), MIT Press, pp 217–244.

[14] MAGMA Computational Algebra System
`http://magma.maths.usyd.edu.au/magma/`

[15] Menju, S., Sakai, K., Sato,Y. and Aiba,A. (1993). A Study on Boolean Constraint Solvers. Constraint Logic Programming Selected Research The MIT Press, pp 253–267.

[16] Montes, A. (2002). A new algorithm for discussing Gröbner bases with parameters. J. Symb. Comp. 33/2, pp 183–208.

[17] Manubens, M. and Montes, A. (2006). Improving DISPGB algorithm using the discriminant ideal. J. Symb. Comp. 41/11, pp 1245–1263.

[18] Noro, M. et al. (2009). A Computer Algebra System Risa/Asir. `http://www.math.kobe-u.ac.jp/Asir/asir.html`.

[19] Brickenstein, M. and Dreyer,A.(2009). A framework for Gröbner-basis computations with Boolean polynomials. J. Symb. Comp.44/9 pp 1326–1345.
PolyBoRi Polynomials over Boolean Rings.
http://polybori.sourceforge.net/
[20] Rudeanu, S. Boolean functions and equations. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1974.
[21] Sato, Y., Nagai, A. and Inoue, S.(2008). On the Computation of Elimination Ideals of Boolean Polynomial Rings. Springer LNAI 5081, pp 334–348.
[22] Sakai, K. and Sato, Y. (1988). Boolean Gröbner bases. ICOT Technical Momorandum 488. http://www.jipdec.or.jp/archives/icot/ARCHIVE
/Museum/TRTM/tm0488.htm
[23] Sakai, K., Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613. http://www.jipdec.or.jp/archives/icot
/ARCHIVE/Museum/TRTM/tr0613.htm
[24] Sato, Y. et al.(1995). Set Constrains Solvers(Prolog version).
http://www.jipdec.or.jp/archives/icot/ARCHIVE/Museum/FUNDING
/funding-95-E.html
[25] Sato, Y.(1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. Proceedings of ISSAC 1998, pp 317–321.
[26] Sato, Y. et al.(1998). Set Constrains Solvers(Klic version).
http://www.jipdec.or.jp/archives/icot/ARCHIVE/Museum/FUNDING
/funding-98-E.html
[27] SINGULAR http://www.singular.uni-kl.de/
[28] Suzuki, A. and Sato, Y. (2003). An Alternative approach to Comprehensive Gröbner Bases. J. Symb. Comp. 36/3-4, 649–667.
[29] Suzuki, A. and Sato, Y. (2006). A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. In Proceedings of ISSAC 2006, pp 326–331.
[30] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings. In Davenport Ed., editor, *EUROCAL'87*, pp 336-347. Springer LNCS 378.
[31] Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.