An efficient implementation of Boolean Gröbner Bases of a power set algebra

Akira Nagai
nagai.akira@lab.ntt.co.jp
NTT Secure Platform Laboratories
Japan

Yosuke Sato
ysato@rs.kagu.tus.ac.jp
Tokyo University of Science
Japan

Abstract

An implementation method of Boolean Gröbner bases of a powerset algebra introduced in [14] is optimized for developing a software in the computer algebra system SageMath using the PolyBoRi library. Our software achieves tremendous speed-up comparing to our previous implementation in the computer algebra system Risa/Asir. It enables us to have a first-ever real time symbolic computation Sudoku solver by Gröbner bases. It also leads us to correct errors on the data of a mathematical hierarchy of Sudoku puzzles reported in [15].

1 Introduction

A residue class ring $\mathbf{B}[X_1, \ldots, X_n]/\langle X_1^2 + X_1, \ldots, X_n^2 + X_n\rangle$ over a Boolean ring $\mathbf{B}$ is called a *Boolean polynomial ring*. A Gröbner basis in a Boolean polynomial ring is called a *Boolean Gröbner basis*, which is first introduced in [3] together with its computation algorithm. An ideal in a polynomial ring over the Galois field $\mathbb{GF}_2$ is 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. When the Boolean ring $\mathbf{B}$ is a power set algebra, Boolean Gröbner bases are of great importance for solving certain types of combinatorial problems. Since we need a special data structure to encode a Boolean ring of a power set algebra, it is not straightforward to implement the computation of Boolean Gröbner bases in a general purpose computer algebra system. In fact the first implementation was done in the logic programing languages Prolog and Klic [4, 5]. When a Boolean ring $\mathbf{B}$ is the simplest power set algebra, i.e., the Galois field $\mathbb{GF}_2$ with characteristic 2, we can easily compute Boolean Gröbner bases in most computer algebra system with a facility to compute Gröbner bases in a polynomial ring over a finite field.

By the technique introduced in [14], we can now compute Boolean Gröbner bases of an arbitrary finite powerset algebra by the computation of Boolean Gröbner bases of $\mathbb{GF}_2$. This method is implemented in the computer algebra system Risa/Asir [10]. It brings us a much faster program than those of [4, 5], which enables us to obtain the recent work of Sudoku puzzles [15]. Though the purpose of the application of Boolean Gröbner bases to Sudoku puzzles is not making a fast solver, the program can solve any Sudoku puzzle in acceptable length of time, while other existing Sudoku solvers by the computation of Gröbner bases such as [11, 12] can solve only limited types of puzzles. Nevertheless, we can not say it is a real time Sudoku solver since the program takes more than 10 seconds for solving most puzzles by a standard laptop computer.

In this paper we describe our implementation of Boolean Gröbner bases of a powerset algebra in the computer algebra system SageMath using the PolyBoRi library [1]. Since PolyBoRi has an optimal data structure for the computation of a Boolean polynomial ring over $\mathbb{GF}_2$, our program achieves about 15 times speed-up than the previous program in Risa/Asir. As a result we get a real time symbolic computation Sudoku solver. We have also recomputed s-ranks of 735 Sudoku puzzles treated in [15] and found serious mistakes on the computation data reported in it. The s-rank of a Sudoku puzzle is a mathematical index which represents its level of difficulty that was introduced in [15]. For the computation of s-ranks, we have used a parallel computation facility of SageMath. In our computation environment with 6 core CPU, our program achieves about 15 times speed-up than the previous serial program in Risa/Asir in average.
We put our prototype program as an open software in the following site:

http.www.mi.kagu.tus.ac.jp/˜nagai/BoolGB_Sage/

The paper is organized as follows. In Section 2, we describe how a Boolean ring of a powerset algebra is used for solving certain types of combinatorial problems. In Section 3, we give a quick review of the computation method of Boolean Gröbner bases of a powerset algebra introduced in [14]. In Section 4, we show a performance advantage of SageMath, compared with other computer algebra system. In Section 5, we describe our coding of the computation of Boolean Gröbner bases using the PolyBoRi library. Section 6 contains some data we have obtained through our computation experiments using our program. In Section 7, we correct errors in the recent work of Sudoku puzzles [15].
The reader is referred to [9] for a comprehensive description of Boolean polynomial rings and Boolean Gröbner bases, also to [15] for more detailed description of the application of Boolean Gröbner bases to Sudoku puzzles.

2 Boolean ring of a power set algebra

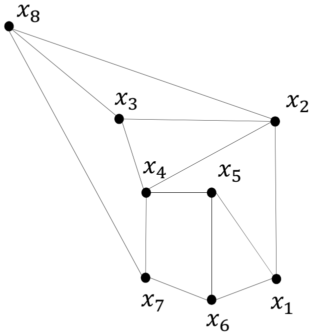
Definition 1 A commutative ring $\mathbf{B}$ with an identity 1 is called *a Boolean ring* if every element a of $\mathbf{B}$ is idempotent, i.e., $a^2 = a$.

$(\mathbf{B},\vee,\wedge,\neg)$ 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. Note that $+$ is nothing but an exclusive OR operator. Note also that $-a = a$.

Definition 2 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. It is called a *powerset algebra* of S.

Definition 3 Let $\mathbf{B}$ be a Boolean ring. A residue class ring $\mathbf{B}[X_1,\ldots,X_n]/\langle X_1^2+X_1,\ldots,X_n^2+X_n\rangle$ modulo 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 m-tuple of elements of $\mathbf{B}$ for some m.
Definition 4 Let I be an ideal of $\mathbf{B}(\bar{X})$. For a subset A of $\mathbf{B}^n$, $V_A(I)$ denotes a subset $\{\bar{a} \in A | \forall f \in I f(\bar{a}) = 0\}$. When $A = \mathbf{B}^n$, $V_A(I)$ is simply denoted by $V(I)$ and called a *variety* of I. We say I is *satisfiable* in A if $V_A(I)$ is not empty. When $A = \mathbf{B}^n$, we simply say I is *satisfiable*.



Example 5 Consider the coloring problem of the above graph by three colors, *green*, *blue* and *red*. Let S be a finite set $\{green, blue, red\}$ and $\mathbf{B}$ be the powerset algebra of S. Let $Sing$ denote the subset of $\mathbf{B}^8$ defined by $Sing = \{(s_1, \ldots, s_8) \in \mathbf{B}^8 |$ each s_i is a singleton$\}$. Without loss of generality we can assume x_1 is assigned to *green* and x_2 is to *blue*. Then the problem is equivalent to computing the variety $V_{Sing}(I)$ for the ideal $I = \langle x_1 + \{green\}, x_2 + \{blue\}, x_1x_2, x_1x_5, x_1x_6, x_2x_3, x_2x_4, x_2x_8, \ldots, x_7x_8 \rangle$ of $\mathbf{B}(x_1, x_2, \ldots, x_8)$.

4				9				
3						1	8	
			5					
		5	8					
	2	9						
					1	7		
		6					5	
					7			
			2					9

Example 6 Consider the above Sudoku puzzle. 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 from 9 candidates $\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}$ and $\{9\}$ so that any distinct two variables which lie on a same row, column or block must be assigned different singletons. 17 variables are assigned singletons $X_{11} = \{4\}, X_{15} = \{9\}, \ldots, X_{99} = \{9\}$ as the initial conditions. Let $\mathbf{B}$ be a powerset algebra of the finite set $\{1, 2, \ldots, 9\}$. This constraint is translated into a system of equations of the Boolean polynomial ring $\mathbf{B}(X_{11}, X_{12}, \ldots, X_{99}) = \mathbf{B}(\bar{X})$ as follows:

(1) $X_{11} + \{4\} = 0, X_{15} + \{9\} = 0, \ldots, X_{99} + \{9\} = 0$.
(2) $X_{ij}X_{i'j'} = 0$ for each pair of distinct variables $X_{ij}, X_{i'j'}$ which lie on a same row, column or block.
(3) $\sum_{(i,j)\in A} X_{ij} + 1 = 0$ where A is a set of indices lying on a same row, column or block. (There are 27 such A's. Remember that $1 = \{1, 2, \ldots, 9\}$.)

Let I be the ideal of $\mathbf{B}(\bar{X})$ generated by the corresponding polynomials of (1),(2) and (3). Let $Sing$ denote the subset of $\mathbf{B}^{81}$ defined by $Sing = \{(s_1, s_2, \ldots, s_{81}) \in \mathbf{B}^{81}|$ each s_i is a singleton $\}$. Then the puzzle is equivalent to computing the variety $V_{Sing}(I)$.

The above examples are so-called *singleton set constraints.* We can handle such a constraint by the computation of Boolean Gröbner bases of a finite powerset algebra. See [15] for more details.

3 Computation of Boolean Gröbner bases of a finite powerset algebra

Let S be a finite set and k be its cardinality. Then the Boolean ring $\mathbf{B}$ of the powerset algebra $\mathcal{P}(S)$ is isomorphic to the direct product $\mathbb{GF}_2^k$. More precisely, let $S = \{a_1, a_2, \ldots, a_k\}$ then the isomorphism θ from $\mathcal{P}(S)$ to $\mathbb{GF}_2^k$ is defined by $\theta(A) = (e_1, e_2, \ldots, e_k)$ for each $A \subseteq S$, where $e_i = 1$ if $a_i \in A$ and $e_i = 0$ if $a_i \notin A$ for each $i = 1, \ldots, k$.

For an element $v \in \mathbb{GF}_2^k$, $\pi_i(v)$ denotes the i-th component of v. This projection is naturally extended to a Boolean polynomial of $\mathbb{GF}_2^k(\bar{X})$. The following theorem reduces the computation of a Boolean Gröbner basis of a Boolean polynomial ring $\mathbb{GF}_2^k(\bar{X})$ to the computation of Boolean Gröbner bases of $\mathbb{GF}_2(\bar{X})$.

Theorem 7 In a Boolean polynomial ring $\mathbb{GF}_2^k(\bar{X})$, let G be a finite set of Boolean closed polynomials. Then, G is a (reduced) Boolean Gröbner basis of an ideal I in $\mathbb{GF}_2^k(\bar{X})$ if and only if $\pi_i(G) = \{\pi_i(g)|g \in G\} \setminus \{0\}$ is a (reduced) Gröbner basis of the ideal $\pi_i(I) = \{\pi_i(f)|f \in I\}$ in $\mathbb{GF}_2(\bar{X})$ for each $i = 1, \ldots, k$.

For each $i = 1, \ldots, k$, define a map ϕ_i from $\mathbb{GF}_2$ to $\mathbb{GF}_2^k$ by $\phi_i(0) = (0, \ldots, 0)$ and $\phi_i(1) = (e_1, \ldots, e_k)$ where $e_i = 1$ and $e_j = 0$ for any j such that $j \neq i$. It is also naturally extended to a map from $\mathbb{GF}_2(\bar{X})$ to $\mathbb{GF}_2^k(\bar{X})$.

Algorithm: Boolean GB
input: F a finite subset of $\mathbb{GF}_2^k(\bar{X})$ and a term order $>$ on $T(\bar{X})$
output: G a reduced Boolean Gröbner basis of $\langle F\rangle$ w.r.t. $>$
For each $i = 1, \ldots, k$ compute the reduced Boolean Gröbner basis G_i of the ideal $\langle \pi_i(F)\rangle$ in $\mathbb{GF}_2(\bar{X})$. Set $G = \cup_{i=1}^k \phi_i(G_i)$.

In order to get a stratified Boolean Gröbner basis, we further need the following manipulation.

Algorithm: Stratification
input: G a reduced Boolean Gröbner basis in $\mathbb{GF}_2^k(\bar{X})$

output: G' a stratified Boolean Gröbner basis
Let $\{t_1, \dots, t_s\}$ be the set of all leading terms of some polynomial in G. For each $i = 1 \dots, s$, let $g_i = \sum_{LT(g)=t_i, g \in G} g$. Set $G' = \{g_1, \dots, g_s\}$.

4 Efficient BGB software

In this section, we give the computation data obtained by SageMath, Risa/Asir, Mathemathica, Maple, and Singlar, in order to consider suitable software to compute Boolean Gröbner bases. In the experiments, we used randomly generated 20 examples which include polynomials over $\mathbb{GF}_2$ with 100 variables by using PolyBoRi command "random_element". Most combinatorial problems are consisted of polynomials which have total degree 1 or 2 because the Boolean operations $\vee, \wedge, \neg$ are defined by $a \vee b = a + b + a \cdot b, a \wedge b = a \cdot b, \neg a = 1 + a$. In fact, polynomials of Example 5 and 6 are constructed of a linear combination of monomials have total degree 1 or 2. In our experiments, we therefore randomly generated polyomials have total degree 1 or 2 like Example 8, 9 and 10. All the computations are done by the same computer with the following spec:

OS: Ubuntu 14.04 LTS 64bit, CPU: Intel(R) Core(TM) i7-3970X, Clock: 3.50GHz, Number of Cores: 6, Memory: 64GB.

We compared the following system:

SageMath Version 6.7: PolyBoRi package with heuristic option False. Risa/Asir Version 20140224: "nd_gr" command. Mathemathica Version 10: Modulus 2 options. Maple: Gröbner package with default options. Singular 3-1-6: "std" command. With the exception of SageMath, we add the following polynomials $\{x_1^2+x_1,\ x_2^2+x_2,\ \cdots,\ x_n^2+x_n\}$ to polynomials F in Examples.

Table 1 contains computation time of Gröbner bases (in seconds) of F in examples 8, 9 and 10.

	SageMath	Risa/Asir	Singlar	Mathematica	Maple
Example 8	0.73	0.99	0.27	1723.74	>1 hour
Example 9	3.66	40.49	385.65	>1 hour	>1 hour
Example 10	500.90	> 2 hours	> 2 hours	>2 hours	>2 hours

Table 1: Computation time of Gröbner bases (Sec)

For other 8 examples, a Gröbner basis computation by Risa/Asir, Mathematica, Maple and Singlar did not terminate in hours, whereas SageMath successfully computed.

Example 8 $F = \{x_{17}x_{77} + x_{60}x_{85},\ x_4x_{96} + x_{96}x_{99},\ x_{35}x_{84} + x_{39}x_{59},\ x_{23}x_{58} + x_{61}x_{83},\ x_{35}x_{45} + x_{43}x_{76},\ x_{17}x_{51} + x_{75}x_{85},\ x_{49}x_{73} + x_{70},\ x_{28}x_{50} + x_{35}x_{80},\ x_8x_{30} + x_{14}x_{49},\ x_{35}x_{41} + x_{52}x_{54},\ x_{13}x_{29} + x_{17}x_{28},\ x_{21}x_{72} + x_{39}x_{49},\ x_{22}x_{92} + x_{37}x_{38},\ x_{17}x_{55} + x_{57}x_{98},\ x_{14}x_{72} + x_{32}x_{67},\ x_{25}x_{42} + x_{58}x_{80},\ x_1x_{24} + x_{78}x_{96},\ x_{20}x_{41} + x_{58}x_{84},\ x_{20}x_{47} + x_{36}x_{41},\ x_{46}x_{56} + x_{66}x_{75},\ x_{26}x_{85} + x_{46}x_{100},\ x_{43}x_{60} + x_{44}x_{69},\ x_5x_{82} + x_6x_{27},\ x_{26}x_{94} + x_{30}x_{65},\ x_1x_{88} + x_{54}x_{90}\}$.

Example 9 $F = \{x_{39}+x_{40}x_{76}+x_{45}+x_{52}+x_{93}+x_{94},\ x_{24}+x_{25}x_{62}+x_{25}+x_{51}+x_{72}+x_{80},\ x_{25}x_{71}+x_{25}+x_{32}+x_{38}+x_{69}+x_{90},\ x_5+x_{16}x_{30}+x_{22}+x_{35}+x_{65}+x_{96},\ x_7x_{54}+x_{11}+x_{49}+x_{67}+x_{87}+x_{92},\ x_5x_{53}+x_{17}+x_{37}+x_{74}+x_{76}+x_{90},\ x_{17}+x_{44}x_{66}+x_{61}+x_{65}+x_{74}+x_{89},\ x_{16}+x_{33}+x_{34}+x_{57}x_{69}+x_{59}+x_{73},\ x_{10}+x_{35}x_{41}+x_{51}+x_{59}+x_{100}+1,\ x_2+x_5x_{47}+x_{56}+x_{91}+x_{92}+x_{95},\ x_{15}+x_{30}x_{96}+x_{30}+x_{37}+x_{84}+x_{86},\ x_1+x_{53}+x_{76}x_{88}+x_{76}+x_{85}+1,\ x_{10}+x_{19}x_{22}+x_{35}+x_{50}+x_{58}+x_{92},\ x_{18}+x_{37}+x_{44}+x_{51}x_{59}+x_{59}+x_{77},\ x_{30}+x_{31}x_{73}+x_{38}+x_{45}+x_{78}+x_{89},\ x_{14}+x_{22}+x_{24}+x_{81}x_{98}+x_{92}+x_{98},\ x_{10}x_{31}+x_{19}+x_{39}+x_{40}+x_{41}+x_{44}\}$.

Example 10 $F = \{x_4x_{84} + x_{69}x_{92},\ x_{49}x_{82} + x_{75}x_{89},\ x_{41}x_{73} + x_{58}x_{75},\ x_1x_{43} + x_9x_{50},\ x_2x_{86} + x_{15}x_{79},\ x_{24}x_{34} + x_{45}x_{52},\ x_4x_{48} + x_{22}x_{98},\ x_2x_{23} + x_{51}x_{81},\ x_8x_{77} + x_{10}x_{79},\ x_3x_8 + x_{53}x_{95},\ x_3x_{73} + x_{18}x_{95},\ x_8 + x_{18} + x_{27} + x_{29} + x_{30} + x_{66},\ x_2 + x_9 + x_{63} + x_{73} + x_{79} + x_{97},\ x_{36} + x_{46} + x_{59} + x_{63} + x_{70} + x_{74},\ x_{31} + x_{34} + x_{36} + x_{41} + x_{60} + x_{66},\ x_9 + x_{30} + x_{48} + x_{79} + x_{83} + x_{88},\ x_{26} + x_{47} + x_{67} + x_{85} + x_{88} + x_{100},\ x_1 + x_{42} + x_{53} + x_{55} + x_{86} + x_{98},\ x_{33} + x_{57} + x_{69} + x_{70} + x_{84} + x_{90},\ x_3 + x_{12} + x_{14} + x_{59} + x_{61} + x_{72},\ x_2 + x_{41} + x_{43} + x_{63} + x_{91} + x_{97},\ x_{12} + x_{19} + x_{38} + x_{62} + x_{65} + x_{77},\ x_{20} + x_{32} + x_{36} + x_{50} + x_{98} + 1,\ x_2 + x_4 + x_{17} + x_{40} + x_{85} + x_{92},\ x_{11} + x_{29} + x_{31} + x_{46} + x_{79} + x_{98},\ x_{10} + x_{51} + x_{58} + x_{59} + x_{89} + x_{90},\ x_2 + x_8 + x_{17} + x_{42} + x_{50} + x_{93},\ x_6 + x_{24} + x_{27} + x_{64} + x_{86} + x_{90},\ x_1 + x_6 + x_{47} + x_{67} + x_{74} + x_{85},\ x_{26} + x_{40} + x_{54} + x_{57} + x_{68} + x_{89},\ x_7 + x_{51} + x_{53} + x_{92} + x_{94} + x_{98}\}$.

5 Coding in SageMath

Our program to compute Boolean Gröbner bases of a finite powerset algebra $\mathcal{P}(\{s_1, \ldots, s_k\})$ has the following rather simple shape.

```
def bgb(Polys,Vars,Eles):
    B=BooleanPolynomialRing(len(Vars)+len(Eles),Eles+Vars,order='lex')
    BPolys=(B.ideal(Polys)).gens()
    BEles=(B.ideal(Eles)).gens()
    Polys_set=divide(BPolys,Eles)
    Bgb_Set=bgb_comp(Polys_set,Vars,Eles)
    Ele_Polys=mulatom(Bgb_Set,BEles)
    Bgb=stratify(Ele_Polys,Eles)
    return Bgb
```

A Boolean polynomial of $\mathcal{P}(\{s_1, \ldots, s_k\})(\bar{X})$ is represented by a Boolean polynomial of $\mathbb{GF}_2(s_1, \ldots, s_k, \bar{X})$ considering $s_1, \ldots, s_k$ as indeterminates. For example, a Boolean polynomial $\{green, red\}X_1 + \{blue\}X_2$ is represented by a polynomial $(green + red) * X_1 + blue * X_2$. We input a list of such represented Boolean polynomials in `Polys`, a list of variables, i.e., $\bar{X}$ in `Vars` and a list of elements, i.e., $s_1, \ldots, s_k$ in `Eles`. `BooleanPolynomialRing` is a PolyBoRi command which defines a Boolean polynomial ring $\mathbb{GF}_2(\bar{X}, s_1, \ldots, s_k)$. For the input F of `Polys`, `divide` computes $\pi_i(F)$ for each $i = 1, \ldots, k$. `bgb_comp` computes a reduced Gröbner basis G_i of the ideal $\langle \pi_i(F) \rangle$ in $\mathbb{GF}_2(\bar{X})$ for each $i = 1, \ldots, k$, which uses the PolyBoRi program `groebner_basis` to compute Gröbner bases of $\mathbb{GF}_2$. `mulatom` is a program to compute $\pi_i^{-1}(G_i)$. Finally `stratify` compute the stratified Boolean Gröbner basis G'.

The following is a computation example of a Boolean Gröbner basis by our program. It compute the stratified Boolean Gröbner basis $\{x + \{s_1\}, y + \{s_2\}\}$ of the ideal $\langle (1 + \{s_1, s_2\})(XY + X + Y), \{s_1\}X + \{s_1\}, \{s_2\}Y + \{s_2\}, XY \rangle$ in a Boolean polynomial ring $\mathcal{P}(\{s_1, s_2\})(x, y)$ w.r.t. a lex order such that $x > y$.

```
% sage
sage: load("bgb.sage")
sage: var("x,y,s1,s2")
(x, y, s1, s2)
sage: bgb([(1+s1+s2)*(x*y+x+y),s1*x+s1,s2*y+s2,x*y],[x,y],[s1,s2])
[x + s1, y + s2]
```

6 Computation Data

We give the computation data obtained by our program of SageMath and the previous program of Risa/Asir [10]. (For the computation of s-ranks, we have fixed its bug.) We also optimized programs of both Risa/Asir and SageMath for Sudoku puzzle. All the computations are done by the same computer.

Table a contains average time (in seconds) of 10 puzzles in the Sudoku book High and UltraHard [17] for obtaining a solution of a puzzle. These puzzles have a property of *solvable* introduced in [15]. Each computation is done serially.
Table b contains average time (in seconds) of 10 puzzles in the Sudoku book High and UltraHard [17] for obtaining s-rank of a puzzle. Each computation of SageMath is done in parallel.

	SageMath (Serial)	Risa/Asir (Serial)
High	0.64	9.44
UltraHard	0.77	11.28

(a) Solving time (Sec)

	SageMath (Parallel)	Risa/Asir (Serial)
High	1.90	24.7
UltraHard	8.38	120.78

(b) Computation time of s-rank (Sec)

We put snapshots of the computations of the following puzzles by SageMath programs. `S50_1` is basic solvable, `S60_1` has a s-rank 1.

		9	3	8	4	2		
	8			1			3	
3				5				8
9				2				3
1				7				6
8			4		5			2
4		3				1		7
	2						9	
		8	6	4	1	3		

S50_1

		8	3					
	9			8		5	3	
	6			1	9			7
		4	7		3			5
	7	9				6	4	
2			6		8	1		
5			9	7			6	
	4	6		3			9	
					4	3		

S60_1

```
sage: S=sudoku_solve(S50_1)
This is solvable.
   1  2  3  4  5  6  7  8  9
1 [6, 7, 9, 3, 8, 4, 2, 5, 1]
2 [2, 8, 5, 7, 1, 6, 4, 3, 9]
3 [3, 1, 4, 2, 5, 9, 7, 6, 8]
4 [9, 4, 6, 1, 2, 8, 5, 7, 3]
5 [1, 5, 2, 9, 7, 3, 8, 4, 6]
6 [8, 3, 7, 4, 6, 5, 9, 1, 2]
7 [4, 6, 3, 5, 9, 2, 1, 8, 7]
8 [5, 2, 1, 8, 3, 7, 6, 9, 4]
9 [7, 9, 8, 6, 4, 1, 3, 2, 5]
S50_1: Comp time  0.671790838242
```

```
sage: S=srank(S60_1)
This is NOT solvable.
   1  2  3  4  5  6  7  8  9
1 [4, 5, 8, 3, 2, 7, 9, 1, 6]
2 [7, 9, 1, 4, 8, 6, 5, 3, 2]
3 [3, 6, 2, 5, 1, 9, 4, 8, 7]
4 [6, 1, 4, 7, 9, 3, 8, 2, 5]
5 [8, 7, 9, 1, 5, 2, 6, 4, 3]
6 [2, 3, 5, 6, 4, 8, 1, 7, 9]
7 [5, 8, 3, 9, 7, 1, 2, 6, 4]
8 [1, 4, 6, 2, 3, 5, 7, 9, 8]
9 [9, 2, 7, 8, 6, 4, 3, 5, 1]
S60_1: Comp time 0.777539014816

S-Rank : 1
Comp time of a basic strategy 0.742350101471
Comp time of BR polynpmials 0.231873035431
Comp time of S-rank(SUM) 0.974223136902
```

7 Hierarchy of Sudoku puzzles

In this section, we propose a new hierarchy for the data reported in [15] which is found errors and corrected by our program. We use the same notations given in Example 2. The reader is referred to [15] for s-rank and $BR_k(J)$.

In [15], s-ranks of 525 Sudoku puzzles contained in the series of Sudoku books (named High, SuperHigh, Hard, SuperHard and UltraHard) [17] are reported as in the following table.

s-rank	0	1	2	3	4	5	∞
High	84	3	10	7	1	0	0
SuperHigh	58	9	22	12	4	0	0
Hard	39	15	21	17	8	4	0
SuperHard	17	13	32	24	19	1	0
UltraHard	11	15	22	21	21	9	6

We have recomputed them by our program. The results are as follows.

s-rank	0	1	2	∞
High	84	21	0	0
SuperHigh	58	47	0	0
Hard	40	65	0	0
SuperHard	17	86	2	0
UltraHard	13	90	2	0

Our new data shows that we cannot categorize Sudoku puzzles in terms of their s-ranks. In order to give a finer hierarchy, we define two numbers ‘A’ and ‘B’. ‘A’ means the numbers of solutions which have already gotten for the element which polynomials contained in $BR_k(J)$ have, i.e., 9> A ≥ 0. When A $= 0$ and we cannot construct $BR_k(J)$, then we up s-rank. ‘B’ means the numbers of Boolean Gröbner bases we need compute for getting a maximal ideal, i.e., B > 0. The following table contains an obtained data by our program. In the table, puzzles are ordered from right to left according to our mathematical levels of difficulty.

s-rank	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2
A	-	6	6	4	4	4	4	4	2	2	2	2	2	4	4	2
B	-	1	2	1	2	3	4	5	1	2	3	4	5	3	4	2
High	84	1	1	10	4				2	2						
SuperHigh	58	17		22	2	2			3	1						
Hard	40	10		28	5	1		1	13	6			1			
SuperHard	17	4	1	38	11	3			15	13			1	1		1
UltraHard	13	2		29	9	4	2		21	14	6	3			1	1

8 Conclusions and Remarks

For only solving combinatorial problems such as Sudoku puzzles, symbolic computation of Boolean Gröbner bases is too heavy. In fact, a Sudoku puzzle can be formulated in a Boolean polynomial ring of $\mathbb{GF}_2$ using 729 variables. This approach is hired for Sudoku solvers by SAT. They can solve any Sudoku puzzle in a second, while symbolic computation for such a formulation is too heavy even for PolyBoRi. However, this formulation cannot decide the level of difficulty of a Sudoku puzzle. Our approach by symbolic computation is an ideal tool for deciding the s-rank of a Sudoku puzzle.

When a given Sudoku puzzle is not basic solvable, for computing its s-rank we need computations of many Boolean Gröbner bases. For such a computation, parallel computation is efficient as is shown in Section 6. For very tough Sudoku puzzles such as the one introduced in [16], we need long computation even by our parallel program. Distributive computations by many computers could gain much speed-up, although we have not done this computation yet.

We also have some problems besides Sudoku puzzles for which our BGB algorithm is superior to standard algorithms for our future work.

References

[1] Brickenstein, M., Dreyer, A., 2009. A framework for Gröbner -basis computations with Boolean polynomials. J. Symbolic Comput.44 (9), 1326-1345. PolyBoRi Polynomials over Boolean Rings.
http://polybori.sourceforge.net/.

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

[3] Sakai,K. and Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613.

[4] Sato,Y.(1996). Set Constraint Solvers(Prolog Version).
http://www.jipdec.or.jp/archives/icot/ARCHIVE/Museum/FUNDING/funding-95-E.html

[5] Sato,Y.(1998). Set Constraint Solvers(KLIC Version). http://www.jipdec.or.jp/archives/icot/ARCHIVE/Museum/FUNDING/funding-98-E.html

[6] Sato, Y. and Inoue, S.(2005). On the Construction of Comprehensive Boolean Gröbner Bases. Proceedings of the 7th Asian Symposium on Computer Mathematics(ASCM2005), pp. 145-148.

[7] Sato, Y., Nagai, A. and Inoue, S.(2008). On the computation of elimination ideals of boolean polynomial rings. In: LNCN, vol. 5081. Springer, pp. 334-348.

[8] Inoue, S.(2009). On the Computation of Comprehensive Boolean Gröbner Bases. Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing(CASC 2009), LNCS 5743, pp 130-141, Springer-Verlag Berlin Heidelberg.

[9] Sato, Y. et al.(2011). Boolean Gröbner bases. J. Symbolic Comput.46 (2011), 622-632.

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

[11] Elizabeth Arnold, Stephen Lucas and Laura Taalman, Gröbner basis representations of Sudoku, The College Mathematics Journal, Vol. 41(2), pp. 101-112, 2010

[12] Jesus Gago-Vargas, Isabel Hartillo-Hermoso, Jorge Martin-Morales and Jose Maria Ucha-Enriquez, Sudokus and Grobner bases: not only a divertimento, Proc. Computer Algera in Scientific Computing, LNCS, Vol. 4194, pp.155.165, Springer, 2006

[13] On the Computation of Comprehensive Boolean Gröbner Bases. Proceedings of CASC2009, pp 130-141, Springer LNCS 5743, 2009.

[14] Nagai, A and Inoue, S.(2014). An Implementation Method of Boolean Gröbner Bases and Comprehensive Boolean Gröbner Bases on General Computer Algebra Systems. Proceedings of ICMS2014, pp 531-536, Springer LNCS 8592, 2014.

[15] Inoue, S and Sato, Y. A Mathematical Hierarchy of Sudoku Puzzles and its Computation by Boolean Gröbner Bases. Proceedings of 12th International Conference, AISC2014, pp 88-98 LNAI 8884, 2014.

[16] Challenge your brain: is this the world's hardest Sudoku? http://www.efamol.com/efamol-news/news-item.php?id=10

[17] Gohnai,K., and Cross Word editorial desk.(2008). Number Placement Puzzles(Basic,Middle,High,SuperHigh,Hard,SuperHard, UltraHard), (In Japanese) Kosaido Publishing Co., 2008.

university teaching is predominantly lecture-based, and sometimes students find the transition from secondary school to university difficult.

Curiously, a study some years ago [9] found that Chinese teachers in "lower grades" had more confidence in employing technology than did their US counterparts; the author's interpretation was that Chinese mathematics teachers in lower grades are in general better trained and prepared. Note that technology in the context of this article meant generic technology: AuthorWare, Flash, PowerPoint. The author claimed that Chinese teachers were more keen to use technology for "instruction". There was no indication that teachers would put such technology in the hands of learners.

4 Conclusions

Although there appear differences between the Chinese and Australian attitudes, as evidenced by our survey, the similarities in fact outweigh them. In both countries tertiary mathematics is teacher-centred and syllabus-driven; in both countries the driving force behind most teaching is that of "covering the syllabus"; of "getting through" all the material. This leaves little time for experimentation, and for the use of more student-centred learning models such as problem-based learning, in which one may expect technology to play a major part.

The statistics presented in this paper have been descriptive only; further work will uncover statistical significances, and the degrees to which attitudes in both countries differ.

However, based on the results so far, indications are that academics in both countries have much of the same attitudes: that the use of CAS may well deepen student understanding of mathematical concepts, but there is no room in the syllabi, and little or no local support, for its current use.

References

[1] Peter Gray, "Be Glad for Our Failure to Catch Up with China in Education", *Psychology Today*, May 28, 2013, `http://bit.ly/1HwC2i6`

[2] Sherry Herron, Rex Gandy, Ningjun Ye, and Nasser Syed. "A Comparison of Success and Failure Rates between Computer-Assisted and Traditional College Algebra Sections." *Journal of Computers in Mathematics and Science Teaching* 31, no. 3 (2012) pp249–258

[3] Yueqiang Hu and Lining Hao, "Thoughts on Cultivating Chinese College Students Learning Autonomy in Mathematics", *International Conference on Education Technology and Economic Management (ICETEM)*, 2015, pp145–152

[4] Yeping Li and Rongjin Huang (eds), *How Chinese Teach Mathematics and Improve Teaching*, Routledge, 2013

[5] Xiang Longwan, "Mathematics Education in Chinese Universities", in *The Teaching and Learning of Mathematics at University Levele: An ICMI Study*, ed Derek Holton, Kluwer 2001, pp 45–49

[6] OECD, *PISA 2009 Results: Executive Summary* `http://www.oecd.org/pisa/pisaproducts/46619703.pdf`, 2010

[7] OECD, *PISA 2012 Snapshot of results in mathematics, reading and science*, `http://www.oecd.org/pisa/keyfindings/PISA-2012-results-snapshot-Volume-I-ENG.pdf`, 2013

[8] Kan Wei, "Explainer: what makes Chinese maths lessons so good?" *The Conversation*, March 24, 2014, `http://bit.ly/1HwE7L6`

[9] Zhonghe Wu, "Comparison Study of Teachers Knowledge and Confidence in Integrating Technology into Teaching Mathematics in Elementary School in the U.S. and China", *Journal of Research in Innovative Teaching*, March 2009, Vol 2, pp126–135

[10] Linda Yeung, “Asian students’ superiority at maths due to Confucian focus on hard work”, *South China Morning Post*, December 23, 2013, `http://bit.ly/1HwEyoE`

[11] Dacheng Zhao and Michael Singh. “Why do Chinese-Australian students outperform their Australian peers in mathematics: A comparative case study.” *International Journal of Science and Mathematics Education* Vol 9, no. 1 (2011), pp69–87.

Figure Drawing using KETCindy and its Application to Mathematics Education – Practical example of application of mathematics to mathematics –

Hideyo Makishita
hideyo@shibaura-it.ac.jp
College of Engineering
Shibaura Institute of Technology
Japan

Abstract

Geometric construction normally means generation of a figure suited for given conditions using rulers and a pair of compasses only for a finite number of times. Hereinafter, this is referred to simply as geometric construction. This paper presents a discussion of, in addition to geometric construction, the practice of drawing figures by adding mathematical contents.

When mathematical material is added to geometric construction using rulers and compasses, the use of dynamic geometry (DG) software is one option, whereas KETCindy is used for this study because KETCindy is equipped with DG′s Cinderella as GUI and can be used for drawing figures by Script as CUI. Therefore, mathematically precise figures can be drawn with ease, producing beautiful results. This paper explains figure drawing while the quadratic curve concept is added to geometric construction. The author considers that figure drawing by Script is extremely useful for mathematics education from the viewpoints of application of mathematics to mathematics. This point will be discussed hereinafter.

1 Introduction

Quite a few teachers use LaTeX for the production of handouts to be used for math classes and test questions. The author encountered teachers who were struggling to find and use a system that can output precise and good-looking figures and graphs. The author tested several software packages and now uses KETCindy because it can output precise and good-looking figures and graphs by simple manipulations.

One benefit of KETCindy is that it uses dynamic geometry software Cinderella as the GUI, thereby allowing visual operation. Regarding GUI operation, although operating environments are almost identical to those of other software, an important benefit of Cinderella is that the generation of figures and graphs is made possible by a Character User Interface (CUI).

An additional benefit is that necessary commands and function formulae can be added by programming[1]. Figures in Japanese mathematics[2], which might be drawn only slightly, can be drawn now to a greater degree by the addition of mathematical contents such as quadratic curves.

In addition, with KETCindy, the quality of figures and graphs is equal to or greater than those depicted in the textbook. Furthermore, figures are generated precisely by simple manipulation. Results thus obtained can be output beautifully by LaTeX. Thanks to this system, the quality of figures and graphs used in the data for author′s class and academic papers were improved remarkably. The prime reason why the author uses KETCindy in LaTeX lies here.

All figures shown in Chapter 2 are drawn by KETCindy. The high quality of these figures is readily apparent: they are equal to or greater in terms of quality than those depicted in the textbook. Figure drawing in which Script is used concomitantly is explained taking Japanese mathematics problem as an example. At the same time, the benefits of rendering figures using LaTeX and KETCindy are reported. In Chapter 3, future tasks of mathematics education [1] and fostering of mathematics teacher will be discussed based on the contents of Chapter 2 [2]. In the Appendix, the contents of the Encyclopedia of Geometric Solution [3], which presented the problem consciousness for this paper, are cited.

2 Quality figures drawn using Script and KETCindy

Wasan dealt with numerous problems related to figures [4]. If a drawing meeting with the conditions is given, then the solution itself leading to an answer is not so difficult.

However, in some cases, the generation of a figure is difficult even if the conditions are being given. Here, example problems 1, 2 and 3 shown below are addressed [5]. In fact, the center of circle P can be drawn by adding a quadratic curve concept to figure drawing using rulers and compasses. This illustration presents a quadratic curve drawn using Script. Beautiful drawings can be output by KETCindy.

Ex 1: Find the length of one side of a square when the diameter of circle P is 1.

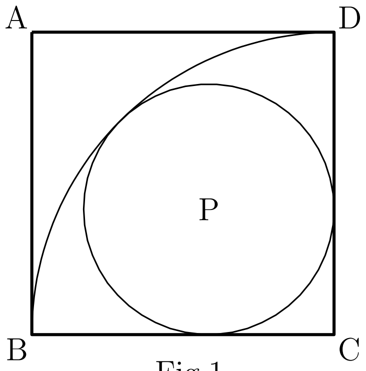


Fig.1.

Ex 2: Find the length of one side of a square when the diameter of circle P is 3.

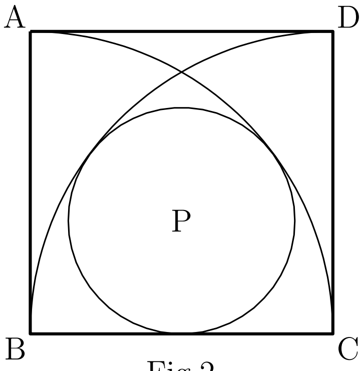


Fig.2.

Ex 3: Two large circles Q and two small circles P are shown in outer circle O. When the diameter of the small circle P is 2, find the diameter of the large circle.

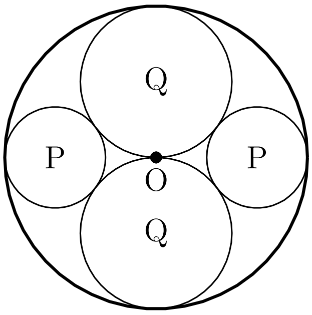


Fig.3.

[1] Function formula capable of creating parabola, ellipsoid, hyperbolic curve, and symbols showing that the lengths of line segments are equal are added by the program.

[2] Japanese mathematics: Wasan which was developed during the Edo Period (1603 – 1867).

2.1 Figure drawing of Example 1: Utilization of a parabola

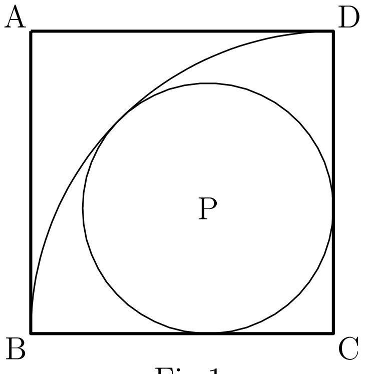


Fig.1.

Example 1 : As illustrated at right, in square ABCD, circle P is inscribed in quadrant C having its center at C, and inscribed on side BC and side CD.
Find the length of one side of the square when the circle diameter is 1.

Answer : The length of one side of the square is $\dfrac{1+\sqrt{2}}{2}$.

2.1.1 Procedures for drawing circle P

Procedures for drawing circle P shown in Example 1 are the following.

1. Center P of the circle passes through intersection E of quadrant C and diagonal line AC.
2. Center P of the circle draws a parabola while E is the focal point and side BC is the directrix.
3. Intersection of a parabola and diagonal line AC is the center P of the circle to be obtained.

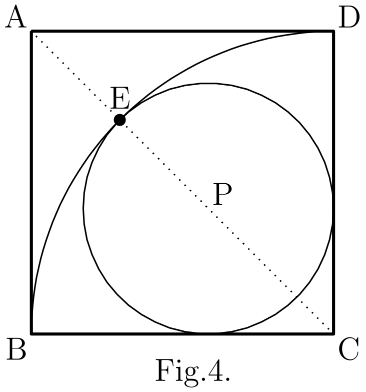


Fig.4.

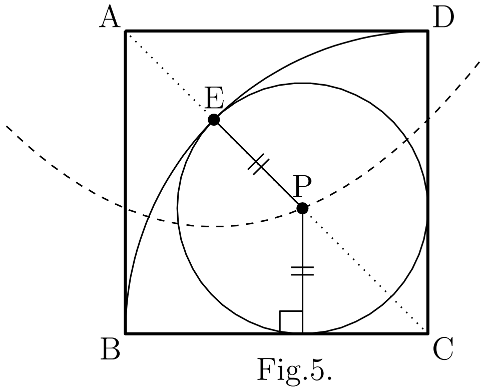


Fig.5.

2.1.2 Example of Script of Example 1

Here, the example of Script of Fig.5 is presented.

Fhead=”Parabola.tex”;	File name: Parabola.tex
Ketinit();	Initialization of KETCindy
Addax(0);	Coordinate axes are not drawn
Listplot([A,B,C,D,A],[”dr,2”]);	Square ABCD is drawn by line 2
Listplot([A,C],[”do,1”]);	Diagonal AC is drawn by dotted line
Circledata([C,B],[”dr,1”,”Rng=[pi/2,pi]”]);	Quadrant C, the part of circle C from $\pi/2$ to π
Parabolaplot(”1”,[E,B,C],[”da,1”]);	Parabola with focal point E and directrix BC
Putintersect(”P”,”rt1para”,”sgAC”);	Intersection P of parabola and diagonal line
Circledata([P,E],[”dr,1”]);	Circle passing through center P and point E
Pointdata(”1”,E,[”size=7”]);	Point E is shown by size 7
Pointdata(”2”,P,[”size=7”]);	Point P is shown by size 7
Letter([A,”nw”,”A”,B,”sw”,”B”,C,”se”, ”C”,D,”ne”,”D”,E,”n2”,”E”,P,”n2”,”P”]);	Points A, B, C, D, E, P are shown
Windispg();	Displayed on the display

Notes : The file name written on the first line and the script shown above are written between the 2nd line and the 13th line. Then the figure can be output by KETCindy on Cinderella, which is the GUI. Furthermore, actual figures can be confirmed by PDF. For the alteration of symbols in the figure and the vertex, the figure might be changed directly returning to Cinderella or changed by Script. At the same time, a tpic file which can be inserted by LaTeX can be generated by the name of the first line. If the file name in the first line is inserted under the layer environment, then a figure can be inserted at the desired point[3]. KETCindy includes expressions of various kinds used in the textbook from mathematics education viewpoints. For example, for the line type, line, dashed line, and dotted line available, each is designated by "dr,n", "da,n" and "do,n" and the thickness can be designated too. The script in the fourth line means a line and thickness 2. The default of the line type and thickness is "dr,1". Function formula Parabolaplot in the seventh line for drawing parabola is added by the program. With KETCindy, function formula and symbol can add functions to be generated as necessary. Those added as necessary are explained hereinafter in each case.

2.1.3 Benefits of using KETCindy

As described previously, the author uses KETCindy to employ mathematically precise figures which are also quality printing materials for mathematics education. Quality printing materials can then be inserted into LaTeX. Comparison of quality of the drawing between DG (a figure of Cinderella is used here) and a figure by KETCindy reveals the difference between the two at a glance.

Furthermore, it might be cited that with KETCindy, the description of Script is mathematical and brief. For example, as represented by the seventh line of parabola Script in the statement above, the focal point and directrix are simply designated. At designation, the focal point and directrix are simply designated by symbols referring to the figure of Cinderella.

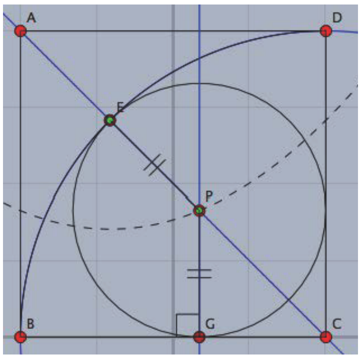


Fig.6.

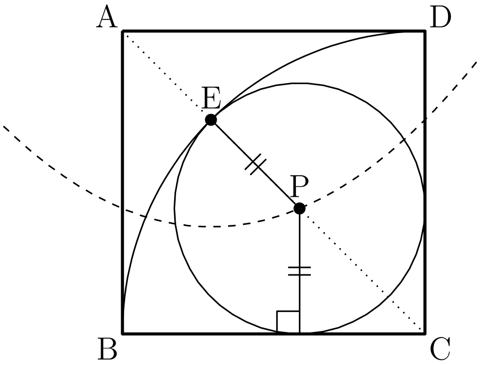


Fig.5.

The following points can be cited as benefits of KETCindy:

1. Cinderella is useful as DG.
2. Precise and quality figures are drawn by DG and might be presented to students as printing materials.
3. Alteration of drawn figures is simple.
4. Program of KETCindy is mathematical and easy to understand.
5. It is freeware and can be introduced easily into school education.

[3] Details are shown in the Appendix provided at the end of this paper.

2.2 Figure drawing of Example 2: Utilization of ellipsoid

Example 2 : As illustrated at right, circle P is in square ABCD and is tangent to two quadrants B and C having its center at point B and point C and to side BC. When the length of the diameter of the circle is 3, find the length of one side of the square.

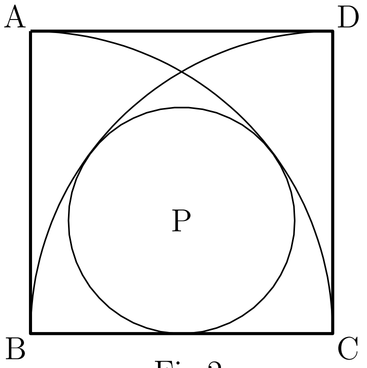


Fig.2.

Answer : The length of one side of the square is 4.

2.2.1 Procedures for drawing circle P

Procedures for drawing circle P shown in Example 2 are the following.

1. Circle P passes through midpoint E of side BC.
2. Circle P is inscribed to quadrant B at point Y.
3. BP + EP = BP + PY = BY = BC (constant).
4. Circle P passes through point E inside of circle B (quadrant B). Therefore, point P is on the ellipsoid having focal point on two points B and E.
5. Center P of the circle is also on the vertical bisector of side BC.
6. Therefore, center P of the circle to be obtained is the intersection of the ellipsoid and vertical bisector.

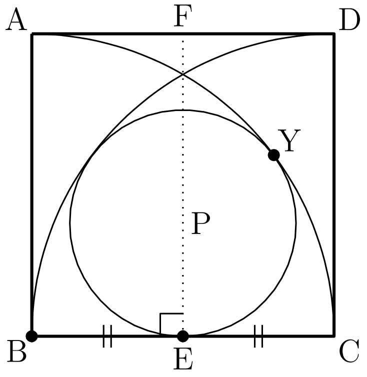


Fig.7.

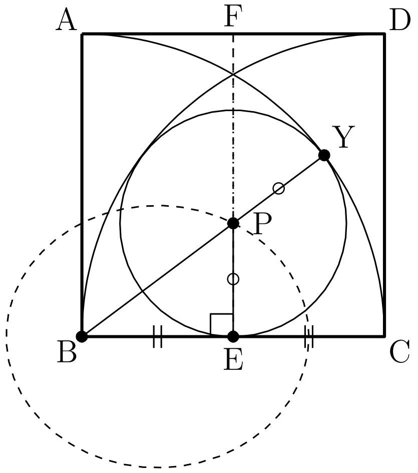


Fig.8.

2.2.2 Example of Script of Example 2

Here, the example of Script of Fig.8 is presented.

4:Listplot([A, B, C, D, A],[”dr,2”]);	Square ABCD is drawn by line 2
5:Circledata([B,C],[”dr,1”,”Rng=[0,pi/2]”]);	Quadrant B, the part of circle B from 0 to $\pi/2$
6:Circledata([C,B],[”dr,1”,”Rng=[pi/2,pi]”]);	Quadrant C, the part of circle C from $\pi/2$ to π
7:Listplot([E,F],[”do,1”]);	Line segment EF: Vertical bisector EF
8:Ellipseplot(”1”,[B,E,|B C|],[”da,1”]);	Ellipsoid having two focal points B and E
9:Putintersect(”P”,”rt1elp”,”sgEF”);	Intersection P of the parabola and segment EF
10:Circledata([P,E],[”dr,1”]);	Circle passing through center P and point E
13:Pointdata(”1”,P,[”size=7”]);	Point P is shown by size 7
15:Drawsegmark(”1”,[B,E],[”Type=2”]);	Mark showing equivalent line segment
16:Drawsegmark(”2”,[C,E],[”Type=2”]);	Mark showing equivalent line segment

Notes : In Example 1, all statements of Script are shown. In Example 2, only major Scripts are shown. Therefore, some line numbers are missing. Drawsegmark shown in the 15th line and 16th line means that two line segments are equal as shown in Fig.7 and Fig.8. Namely, BE = CE. It is visually understood by this symbol that point E is the midpoint of side BC. This expression is used frequently in Japanese mathematics textbooks. In Fig.8, if results show that two points B and E are of focal points, then point P to be obtained should satisfy BP + EP = $2a$ ($2a$ is the sum of distance) as characteristics of the ellipsoid. It is important to recognize that it is the radius of quadrant B. If this is found, |B C| is simply designated in KETCindy. This is similar to vector notation and is mathematically simple.

2.3 Figure drawing of Example 3: Utilization of hyperbola

Example 3 : As illustrated at right, two large circles Q and two small circles P are shown in outer circle O.
When the diameter of small circle P is 2, nd the diameter of the large circle.

Answer : The diameter of the large circle is 3.

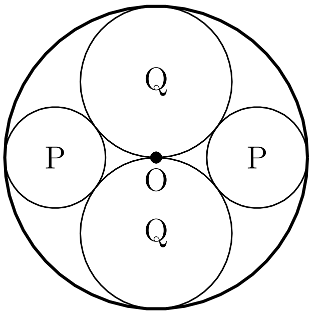


Fig.3.

2.3.1 Procedures for drawing circle P

Procedures for drawing circle P in Example 3 are the following. Two large circles Q are designated as Q1 and Q2. Two small circles P are designated as P1 and P2. Locations of the centers of two large circles Q1 and Q2 might be readily apparent. Procedures drawing center P1 and P2 of two small circles are explained hereunder.

1. Points of tangency of the circle P and circle O are designated respectively as A and B. The line segment AB is a diameter of circle O.
2. Circle P1 and circle Q1 are circumscribed at point Y.
3. Point P1 is outside of circle Q1.
4. |Q1P1 AP1| = |Q1P1 P1Y| = |Q1Y| = |Q1O| (constant).
5. Therefore, P1 is a hyperbola having two focal points of A and Q1.
6. The intersection of hyperbola and diameter AB is center P1 to be obtained.

Similarly, drawing of the center of small circle P2 is obtainable by the hyperbola.

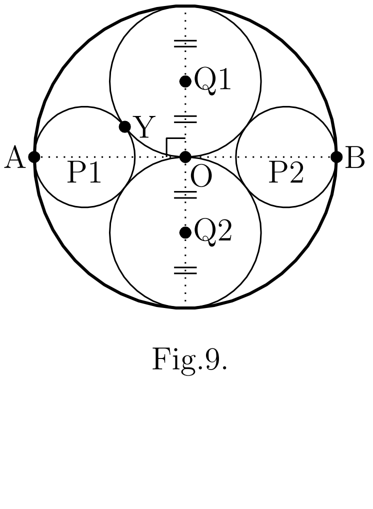


Fig.9.

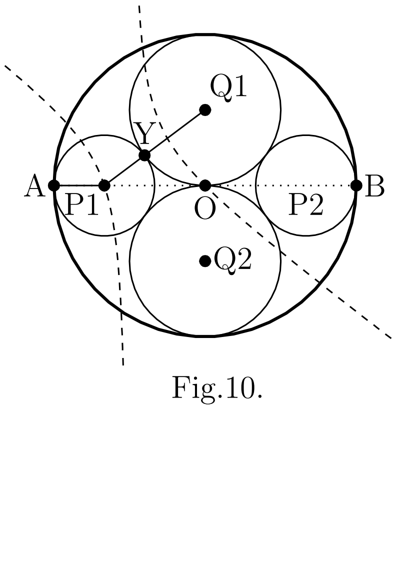


Fig.10.

2.3.2 Example of Script for Example 3

Here, the example of the Script for Fig.10 is presented.

```
 4:Circledata([O,A],[”dr,1”]);               Line type 1 passing through A at center O
 5:Circledata([Q1,O]);                       Circle having its center at Q1 and passing through O
 6:Circledata([Q2,O]);                       Circle having its center at Q2 and passing through O
 7:Listplot([A,B],[”do,1”]);                 Line segment AB is shown by dotted line
 8:Hyperbolaplot(”1”,[A, Q1, |Q1   O|]);     Hyperbola having focal points A and Q1
 9:Putintersect(”P1”,”rt1hyp”,”sgAB”);       Intersection P1 of hyperbola and line segment AB
10:Hyperbolaplot(”2”,[B, Q1, |Q1   O|]       Hyperbola of focal points B and Q1 which is
                              ,[”notex”]);   not shown in TEX
11:Putintersect(”P2”,”rt2hyp”,”sgAB”);       Intersection P2 of hyperbola and line segment AB
12:Circledata([P1,A]);                       Circle having its center at P1 and passing through A
13:Circledata([P2,B]);                       Circle having its center at P2 and passing through B
17:Pointdata(”1”,P1,[”size=7”]);             Point P1 is shown by size 7
```

Notes : Only the major Script relating to Example 3 are shown. Therefore, some line numbers are missing. Regarding the drawing of the hyperbola shown in the eighth line, if results show that in Fig.10 two points of A and Q1 are focal points similarly to Example 2, then the point to be obtained should satisfy $|AP1 \quad Q1P1| = 2a$ (where $2a$ is the difference of distance) as characteristics of the hyperbola. An important matter is recognition that it is the radius of circle Q1. If this is found, then it is designated simply as $|Q1 \quad O|$ in KETCindy.

For drawing of P2, a hyperbola having two focal points of B and Q1 shown in the tenth line should be generated. However, this will complicate Fig.10. Then, “notex” is included, which means that no drawing is provided at the end of the tenth line by the designated option.

3 Summary and Future Tasks

The problems of figure drawing shown in Examples 1, 2 and 3 taken up here are resolved by KETCindy, in which contents of the quadratic curve are added to geometric construction using rulers and a pair of compasses.

Generating a drawing using rulers and a pair of compasses only for a finite number of times is normally designated as geometric construction in the mathematical field. According to the author, generation of a figure by adding mathematical contents to said figure drawing is extended geometric construction. When extended geometric construction is used, a regular heptagon that is impossible to draw accurately can be drawn with extended geometric construction manner by solving high-degree equations. Such educational material is regarded as effective from the perspective of application of mathematics to mathematics. Extended geometric construction is to apply mathematics itself to mathematics and the author considers that from viewpoints of utilization of the learned contents; it is appropriate content for challenge learning in high school and for application of mathematics and mathematical exploration currently proposed.

Next, as represented by KETCindy, a system that can output generated results beautifully as the printed educational material is conducive to mathematics education for pupils and students. Simultaneously, it might be used as a means for research announcements by pupils engaged in

SSH research[4]. The author considers that the application of mathematics to problem-solving is urgent to meet the demands of society as well as curriculum guidelines. Therefore, the author intends to report research outcomes at international conferences in the form of an academic paper under the title of "Application of Mathematics to Mathematics" [1].

With the program used here for figure drawing, parabolas, ellipsoids, and hyperbolas can be generated by designating a focal point and a directrix in a similar manner as the definition of quadratic curves. As a future task, such a program will need Script. To do this, some programming knowledge is necessary for mathematics teachers in secondary school so that they can solve their own problems as well as ICT applications. To that end, the ICT training system will become increasingly important.

Finally, to draw figures meeting the conditions shown in this paper mathematically precisely and beautifully, problems listed in the Encyclopedia of Geometric Solution (1959) [3] should be studied. Then, figures can be drawn easily and mathematically precisely. The author wonders why, although tips for extended geometric construction were listed in the literature published a half century ago, no extended geometric construction idea as introduced by the author has been devised. The reasons for this might be that teaching of quadratic curves was insufficient and that effective application of ICT to mathematics education was not attempted actively. The author feels that ICT is not used extensively in present-day mathematics education. As a future task, we mathematical teachers should apply ICT aggressively. In this case, hardware and software should be modified so that our students might become familiar with them. Teachers should use them to a greater degree. It is desirable that they are able to perform basic mathematical programming of Cinderella and KETCindy introduced in this report. To do so, the author intends to develop and distribute valuable educational materials for mathematics using KETCindy.

Acknowledgements

The author wishes to express his thanks to Prof. Kimio Watanabe (Waseda University) for his valuable advice in writing this paper.

The author is also grateful to KETCindy project members including Prof. Setsuo Takato (Toho University) who provided great assistance in quadratic curve programming.

This work was supported by JSPS KAKENHI Grant No. 26350198.

Appendixes

1. For figure drawing by Script in Examples 1, 2 and 3 in the Encyclopedia of Geometric Solutions [3], reference is made to Item 4 Trajectory of quadratic curve, Section 4 Problems relating to circles, Chapter 5 Trajectory. When results of this problem are used, circle P can be drawn by adding the quadratic curve concept to geometric construction by rulers and a pair of compasses as stated in this paper. Problem numbers 1440, 1444, and 1443

[4] Under the SSH program, in collaboration with universities and other institutions, high schools focus on science and mathematics in conducting experiential learning, research projects and curriculum development. The program aims to foster students with a high level of creativity and a passion for science and technology. [6]

in Encyclopedia of Geometric Solution referred to in this paper are incorporated here as references[5].

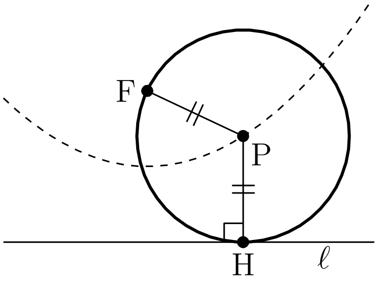
Problems from Encyclopedia of geometric solution

1440. Fixed straight line ℓ and fixed point F outside this straight line are given. Obtain the trajectory of center P of the circle which passes through F and is tangent to ℓ.

1444. Obtain trajectory of center of circle P which passes through fixed point F inside fixed circle F′ and is tangent to fixed circle F′.

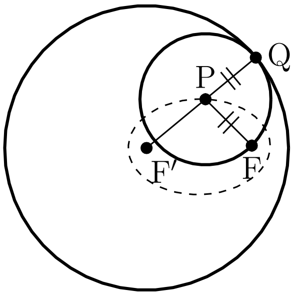
1443. Obtain the trajectory of center of circle P which passes through fixed point F outside fixed circle F′ and which is tangent to fixed circle F′.

The trajectory of circle P is represented by a parabola having focal point F and directrix ℓ, ellipsoid having focal points F′ and F, and hyperbola, respectively. These are drawn by KETCindy.



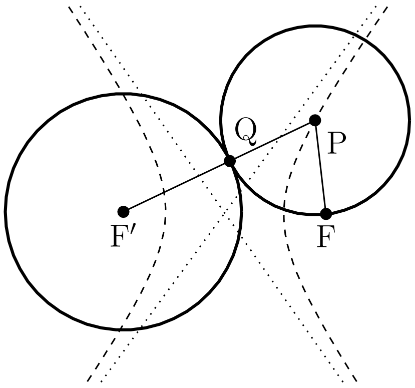
1440.

Point H is the point of contact of circle F and ℓ



1444.

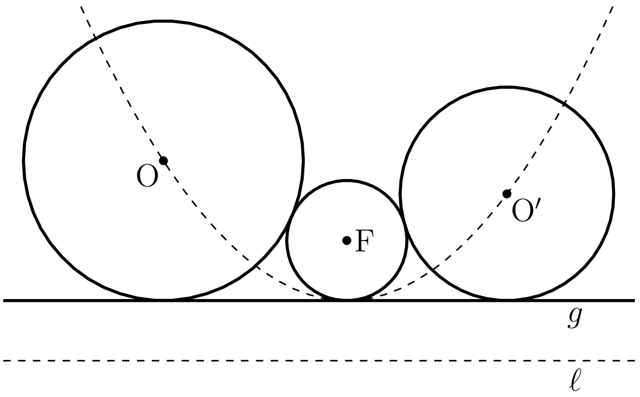
Point Q is the point of contact of circle F′ and circle F



1443.

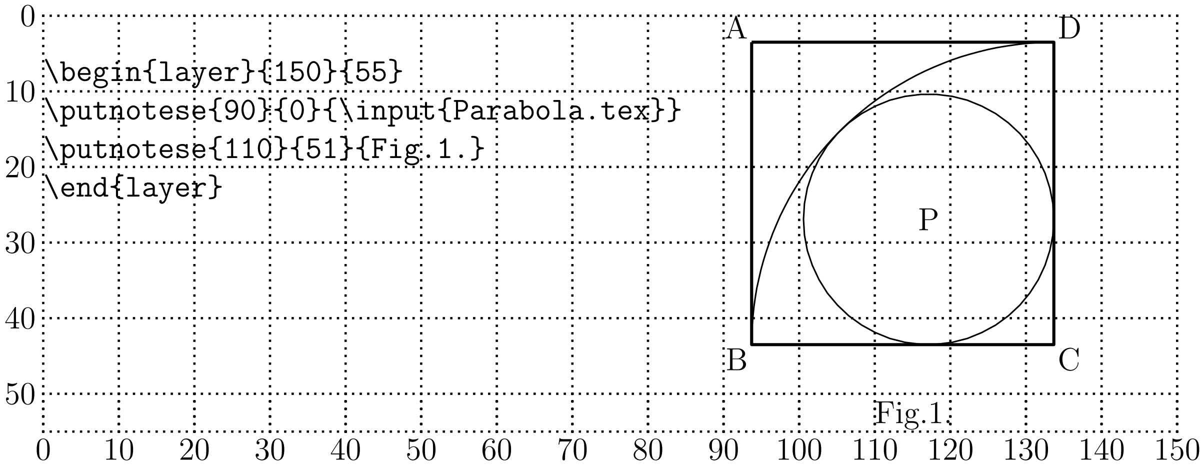
Point Q is the point of contact of circle F′ and circle F

2. The following illustration is used frequently in Wasan. Circle O and circle O′ tangent to common line of tangency g which is tangent to circle F can be drawn. However, point F is the focal point of the parabola shown by dashed line; ℓ shown by dashed line is directrix.



[5] Although these problems ask a student to obtain a trajectory, these are modified to meet the contents of this paper. Figures are of extended geometric construction by Cinderella and ketcindy, and vertex and points are unified to those used in this paper.

3. The author shows how to insert the tpic file in the LaTeX under the layer environment. It is possible to determine the position of the figure as follows.



```
\begin{layer}{150}{55}
\putnotese{90}{0}{\input{Parabola.tex}}
\putnotese{110}{51}{Fig.1.}
\end{layer}
```

The first line means that you display the plane in a grid pattern from point $(0, 0)$ to point $(150, 55)$ by x, y coordinates. The second line means that the file of "Parabola.tex"– Fig.1′s upper-left corner – is placed on the southeast of point $(90, 0)$. When you are satisfied with the position of the figure, you should turn off the grid as below.

```
\begin{layer}{150}{0}*
\putnotese{90}{0}{\input{Parabola.tex}}
\putnotese{110}{51}{Fig.1.}
\end{layer}
```

Therefore, it is possible to obtain the figure of Example 1.

References

[1] Hideyo, Makishita., "Creation of mathematical problems and empirical study of emotional aspect of students", *The Bulletin of the Graduate School of Education of Waseda University, Separate volume, No. 19-1*, 2011a, p.263 - p.274.

[2] Hideyo, Makishita., "Practice with Computer Algebra Systems in Mathematics Education and Teacher Training Courses", *Fourth International Conference, Seoul, South Korea, Springer Lecture Notes Volume 8592, the series Lecture Notes in Computer Science*, 2014a, p.594 - p.600.

[3] Tadashi, Ugaeri. Hitoshi, Hombu. Ichiro, Murase., "Encyclopedia of geometric solution", *Obunsha Co., Ltd.*, 1959a, p.447 - p.448.

[4] Ken'ichi, Sato. and Hiromi, Itoh. and Hideyo, Makishita., "Dojo of mathematical puzzle devoted to shrine or temple", *Kenseisha Co., Ltd.*, 2000a.

[5] Hinoto, Yonemitsu., "The basic problem and solutions of Wasan", *Self-publishing*, 2010a.

[6] Japan Science and Technology Agency., "2011-2012 Guide to the Role of JST and Introduction to Key Programs and Recent Research Cases", *Japan Science and Technology Agency.*, 2012a, p.20.

Teaching Mathematics using Augmented Reality

Janchai YINGPRAYOON, Dr.rer.nat.
Deputy Director, International College,
Suan Sunandha Rajabhat University, Bangkok, THAILAND
Email: janchai@loxinfo.co.th

Abstract

Information technology enables us to develop innovative learning/teaching tools for mathematics education both in the classroom and out-of-school activities. This paper shows a brief potential and challenges of using Augmented Reality (AR) in mathematics education. The learners can view geometrical objects in 3-dimention having better understanding of the structures. Mobile phones or computer tablets can be used to view the 3D geometrical objects using special application software. Autodesk Maya software is used to draw geometrical objects and some AR viewing software can be used to view the objects in 3D. This paper will describe how to develop a simple AR system for the improvement of abilities of learning mathematics. Sample AR materials used for mathematics education at high school as well as university level will also be discussed.

1. Introduction

Augmented Reality in education is relative new but developing rapidly. Sometimes mathematics, especially geometry, in the classroom is difficult to understand because the students have to imagine in a three-dimension way. Virtual Reality (VR) can be used to arouse curiosity and raise motivation of students to enhance the learning process with a high potential.

Azuma [1] gave a good definition of Augmented Reality (AR). AR is a variation of VR. AR allows the users to see the real world with virtual objects composited with the real world. The users can also see geometrical virtual objects like a cube or a cone in 3D superimposed with the pictures of a cube or a cone in 2 dimensions in a textbook. This will help the students to visualize for better understanding.

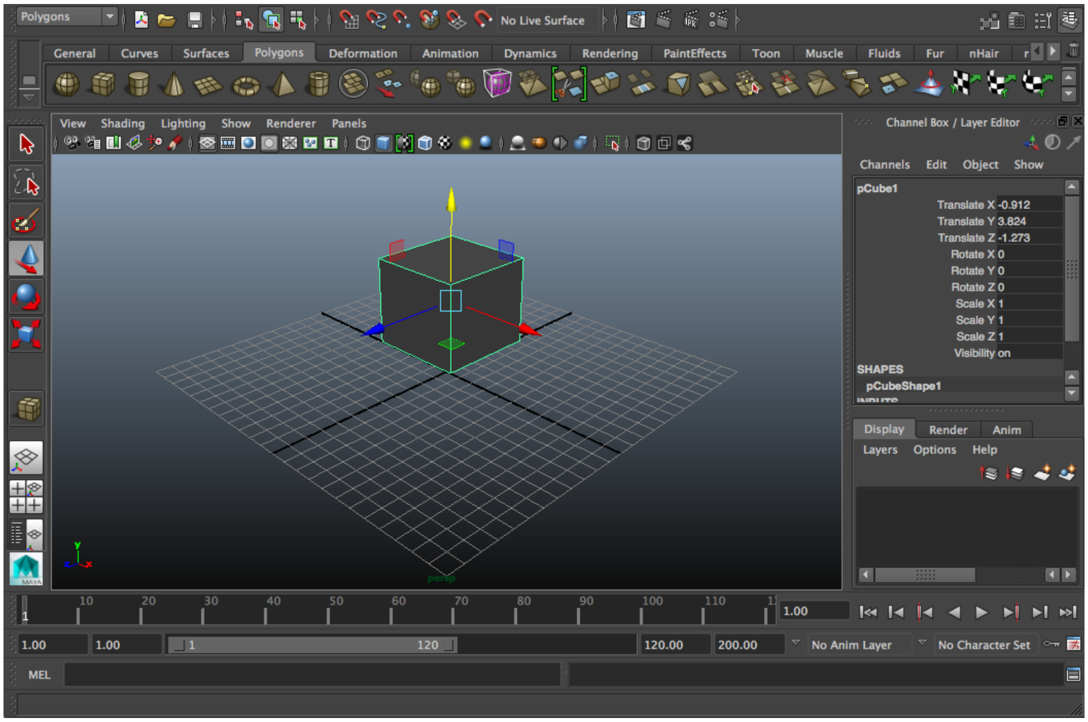
2. Related Work

For better understanding of mathematical models, Virtual Reality (VR) can be used to raise interest of the students as suggested by several authors [9, 11, 12]. Information technology enables us to develop a new approach for mathematics education both in the classroom and out-of-school activities. The important purpose of an educational environment is to introduce social interactions among users in the same physical area [12]. Construction of 3D objects combines four research areas: geometry, pedagogy psychology and augmented reality. There are several researchers developed Augmented Reality from Virtual Reality [2, 3, 4, 13, 6 and many others]. The educational dynamic geometry applications such as Geometer's Sketchpad [5], Cindarella [10], Euklid [8] and Cabri Geometry [7] support two- dimensional geometry only. Augmenter Reality is a rapidly developed with connections of computer graphics and user interface research.

3. Applications

Mobile phones and computer tablets become common tools in daily life. The people always use mobile phones as calculators. Information technology can enables us to develop applications on mobile phones for mathematics education purposes. In order to create 3D objects for mathematics education approaches, we need software for making 3D geometrical models and for scanning or viewing the objects.

There are several software applications using for creating 3D objects in the market. These applications can run on mobile phones or on computers. In this paper I used software Autodesk Maya to create 3D geometrical objects for AR applications. This software can be purchased from personal or commercial uses from website: www.autodesk.com. There is also a student version for educational purposes only.



pCube1

Translate X	-0.912
Translate Y	3.824
Translate Z	-1.273
Rotate X	0
Rotate Y	0
Rotate Z	0
Scale X	1
Scale Y	1
Scale Z	1
Visibility	on

SHAPES
pCubeShape1

Fig.1 Working screen of Autodesk Maya for making a model of a cube.

We have to run the programme Autodesk Maya on a computer to create a model. A type od model can be chosen by clicking a button on the model menu on the top left of the screen. The size and position can be adjusted by dragging a mouse to create the chosen model. The Fig. 1 shows the cube model created by Autodesk Maya. After the model is created, it must be saved using an export command to store the model in a working folder. The model must be saved in the file type

DAE. In this case, the model is saved under the name CUBE.DAE. This model (a cube) will be used to display in a 3D floating on a background in a real world.

In order to construct an AR of the model we created from Autodesk Maya, we need another software to link the model to the background or tracker. The software for Augment Reality can be purchased from http://www.augmentedev.com/. A student version can also be obtained for educational purposes only by contacting the software provider.

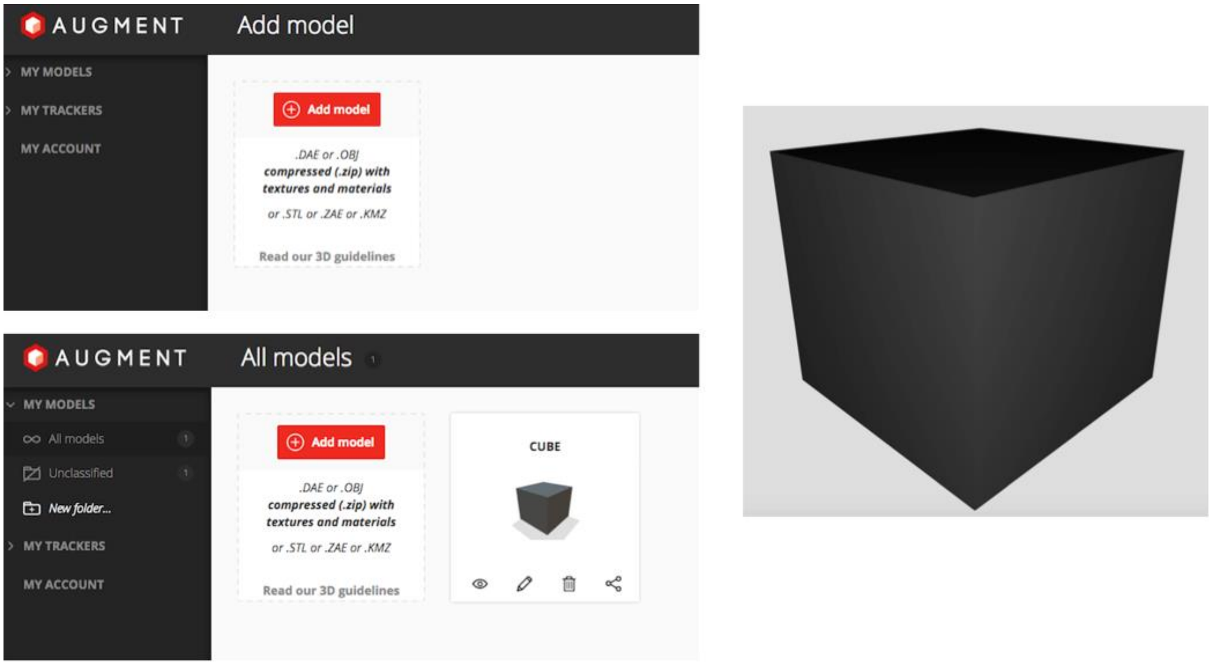
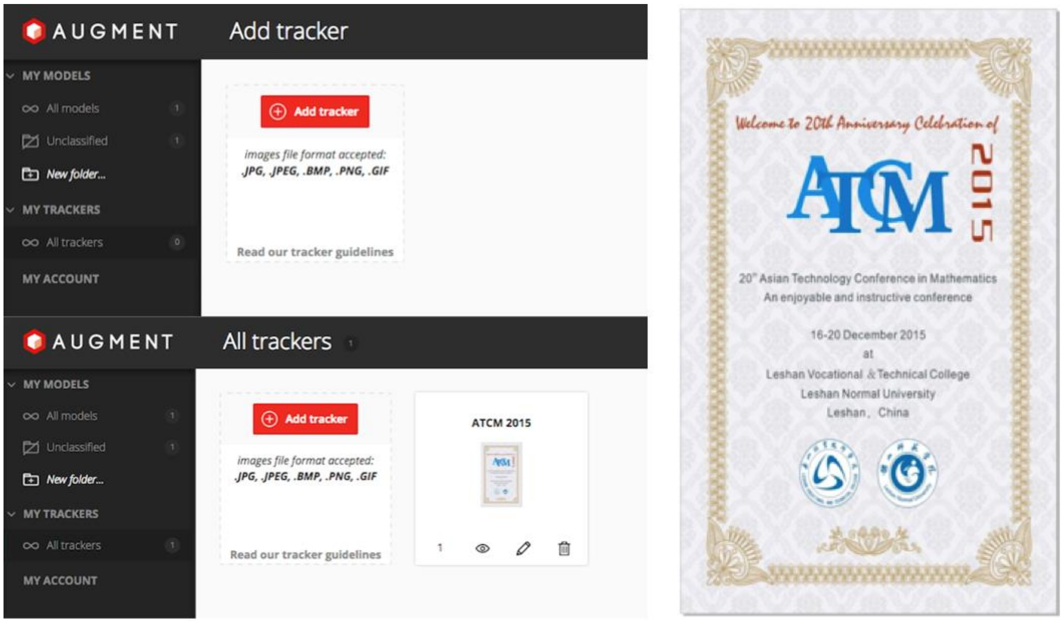


Fig.2 Working screen of Augment for making an AR of a cube model.

When we go to Augment website, we can see the working screen as shown in Fig. 2. The cube model we saved in the working folder of Autodesk Maya has to be added to the AR folder by clicking the button ADD MODEL on the screen. After upload the cube model to Augment folder, a picture of a cube will appear on the screen.

In order to view 3D cube model of AR using a mobile phone or a computer tablet, we need a background picture to be scanned. The background is called tracker.



Welcome to 20th Anniversary Celebration of

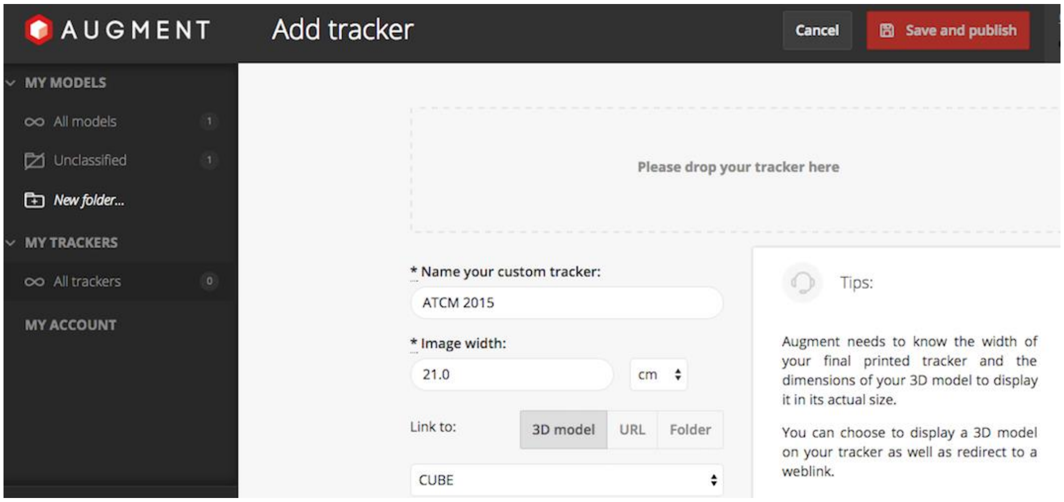
ATCM 2015

20th Asian Technology Conference in Mathematics
An enjoyable and instructive conference

16-20 December 2015
at
Leshan Vocational & Technical College
Leshan Normal University
Leshan，China

Fig. 3 A working screen of Augment for uploading a tracker to AR folder. In this case an ATCM 2015 poster is used as a tracker for AR of a cube model.

We have to prepare a tracker so that it will be used to scan and link with the model that we have in the model folder. An ATCM 2015 poster is used as a tracker for AR of a cube model. In order to upload a tracker photo, we have to click an ADD TRACKER button on the Augment screen. The ATCM tracker is uploaded in to the tracker folder as shown in Fig. 3.



* Name your custom tracker: ATCM 2015

* Image width: 21.0 cm

Link to: 3D model

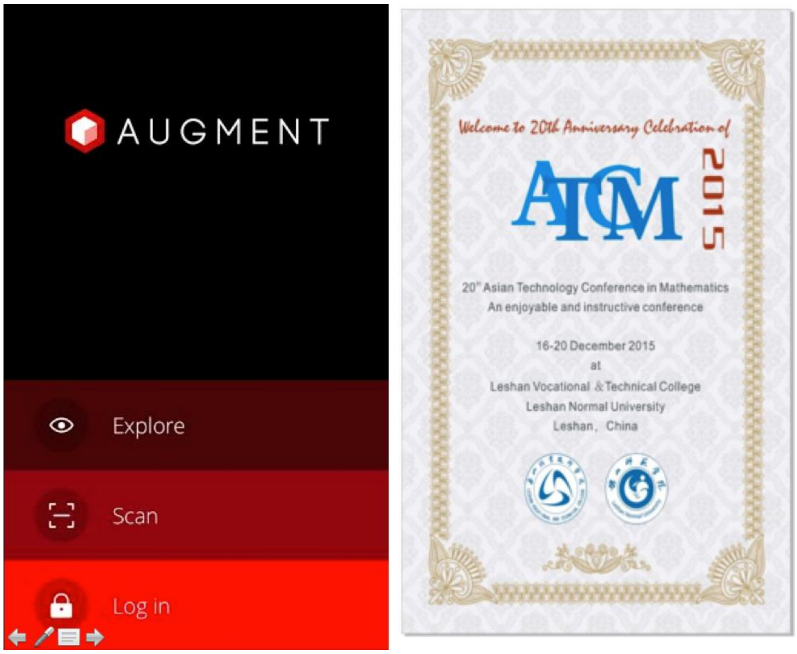
CUBE

Augment needs to know the width of your final printed tracker and the dimensions of your 3D model to display it in its actual size.

You can choose to display a 3D model on your tracker as well as redirect to a weblink.

Fig. 4 Press Save and publish to form the link between the model and the tracker.

The last step to view AR 3D image of the model is to download a special software application for scanning the tracker. In this paper I used application “AUGMENT” for iPhone. When running the application AUGMENT, the menu of the functions will appear as shown in Fig. 5. Press scan button to scan the ATCM 2015 tracker on the left hand side of the Fig. 5.



Welcome to 20th Anniversary Celebration of

ATCM 2015

20th Asian Technology Conference in Mathematics
An enjoyable and instructive conference

16-20 December 2015
at
Leshan Vocational & Technical College
Leshan Normal University
Leshan, China

Fig. 5 Using AUGMENT application to scan the ATCM tracker to view 3D model.

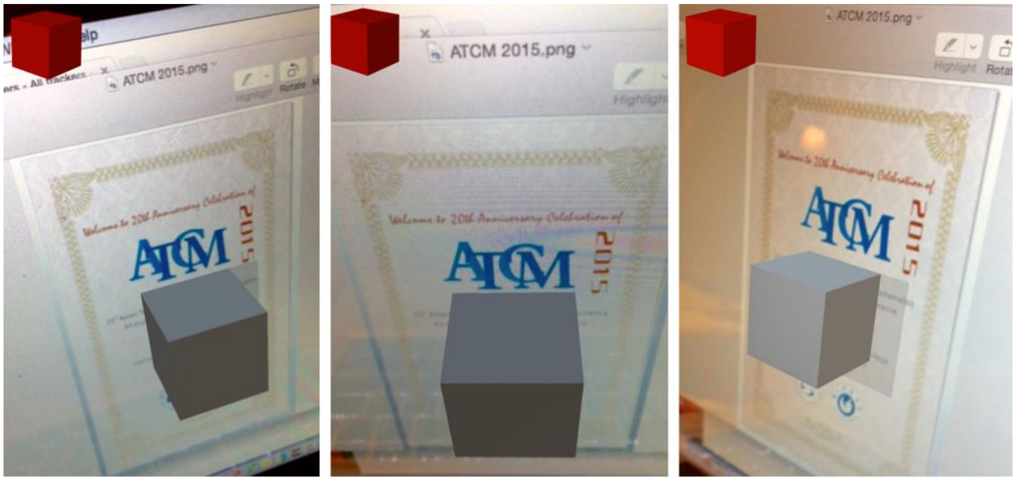
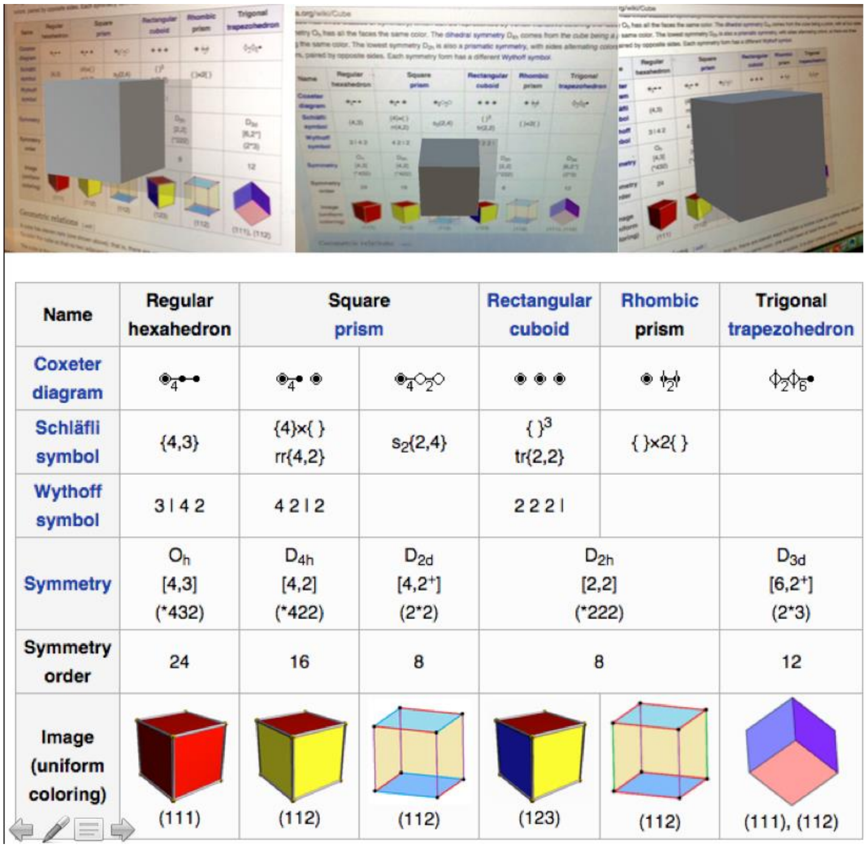


Fig. 6 A cube model viewing from different angles.

After scanning a tracker, a cube model will appear in front of the ATCM tracker when using a mobile phone to scan. 3D images of a cube model can be seen from different positions like a real object floating in the air with tracker background.

4. Using Augmented Reality in the Classroom



Name	Regular hexahedron	Square prism		Rectangular cuboid	Rhombic prism	Trigonal trapezohedron
Coxeter diagram	●4●–●	●4● ●	●4○2○	● ● ●	● ○2○	○2○6●

Schläfli symbol	{4,3}	{4}×{ }
		rr{4,2}
			s_2{2,4}	{ }^{3}
				tr{2,2}
					{ }×2{ }	

Wythoff symbol	3 | 4 2	4 2 | 2		2 2 2 |		
Symmetry	O_h [4,3] (*432)	D_{4h} [4,2] (*422)	D_{2d} [4,2$^+$] (2*2)	D_{2h} [2,2] (*222)		D_{3d} [6,2$^+$] (2*3)
Symmetry order	24	16	8	8		12
Image (uniform coloring)	(111)	(112)	(112)	(123)	(112)	(111), (112)

Fig. 6 Different views of a cube model using a page of textbook as a tracker related to the content in the book.

With the help of AR the teachers can raise interest and motivation of students to enhance the learning process with a high potential for better understanding. It will be more interesting if the teachers can create various AR geometrical models using some pages of the textbook or worksheets as trackers related to the contents being studied. The students can use their own mobile phones or computer tablets to view 3D objects they are studying coming out from the pages and the Virtual objects can be seen from different angles in a 3-dimensional way. The sample of this idea is shown in the Fig. 6.

5. Conclusion

Author conducted several mathematics workshops for teachers and camps for students and was looking for new ways to review math terms for better understanding. Author tried the way using QR codes as well as GIF animator. These ways could make more fun in the classrooms. Augmented Reality (AR) is another way that author tried to make classroom more interesting and fun. This could raise interest and motivation of the learners. Using geometrical pictures in the textbook as trackers to create AR objects, the learners paid more attention to the classroom and they studied more from textbook. Author asked students to create their own AR objects related to the topics they are studying. Some of the students used their own AR objects linking with QR codes as well as GIF animator for their work. The learners shared their AR works among groups. This shows a very strong impact in improving learning environment of mathematics classroom or even self-study anywhere.

References

[1] Azuma, R. A Survey of Augmented Reality. PRESENCE: Teleoperators and Virtual Environments, Vol. 6, No. 4, pp. 355-385, 1997.

[2] Bell JT, and Fogler HS. The Investigation and Application of Virtual Reality as an Educational Tool. In Proceedings of the American Society for Engineering Education 1995 Annual Conference, Session number 2513, Anaheim, CA, 1995.

[3] Bricken M, and Byrne C. Summer Students in Virtual Reality: A Pilot Study on Educational Applications of VR Technology. In A. Wexelblat (Ed.) Virtual Reality, Applications and Explorations. Cambridge, MA: Academic Press Professional, 1993.

[4] Byrne CM. Water on Tap: The Use of Virtual Reality as an Educational Tool. Unpublished Ph.D. thesis, University of Washington, College of Engineering, 1996.

[5] JackiwN.TheGeometer’sSketchpadVersion3.KeyCurriculumPress,Berkeley,1995.

[6] Kaufmann H, Schmalstieg D, and Wagner M. Construct3D: A Virtual Reality Application for Mathematics and Geometry Education. Education and Information Technologies 5:4, pp. 263-276, 2000.

[7] Laborde JM, and Bellemain F. Cabri-Geometry II. Texas Instruments. Copyright Texas Instruments and Université Joseph Fourier, CNRS, 1998. URL: http://www-cabri.imag.fr/index-e.html

[8] MechlingR.EuklidDynageo,2000.URL:http://www.dynageo.com

[9] Pantelidis, V. S. Reasons to Use Virtual Reality in Education, VR in the Schools 1(1), 1995. URL: http://www.soe.ecu.edu/vr/reas.html (Revised 2000)

[10] Richter-Gebert J, and Kortenkamp UH. The Interactive Geometry Software Cinderella: Version 1.2 (Interactive Geometry on Computers), 1999. URL: http://www.cinderella.de/

[11] Roussos, M., Johnson, A., Moher, T., Leigh, J., Vasilakis, C., and Barnes, C. Learning and Building Together in an Immersive Virtual World. PRESENCE 8(3), pp. 247-263, MIT Press, June 1999.

[12] Winn, W. A Conceptual Basis for Educational Applications of Virtual Reality, Technical Report TR 93-9: http://www.hitl.washington.edu/publications/r-93-9/, 1993.

[13] Winn W. The Impact of Three-Dimensional Immersive Virtual Environments on Modern Pedagogy. HITL Technical Report R-97-15. Discussion paper for NSF Workshop. Human Interface Technology Laboratory, University of Washington, 1997.