Complexity of the Membership Question

Aviezri S. Fraenkel
Computer Science and Applied Mathematics
Weizmann Institute of Science
Rehovot, Israel

Two Parts

This talk consists of 2 parts: background and new results.

The background material is known.

But since it's not all that well-known, I thought it would be best to mention it.

Genesis: Nov 2006, Grenoble

- At that time and place, there was the Ph.D. defense of Eric Duchene.
- One of Eric's games was a variation of Wythoff's game, and 4 of us, who worked together on some related problems for a few days after the defense, could get no handle on the problem..
- I thought of solving the problem approximately. I had similar thoughts before.
- Details follow below.

The Idea of this Talk

Provide a probabilistic strategy for impartial combinatorial games whose exact strategy is known, but it's too hard to compute.

To the best of my knowledge, this is the first result in this direction.

There is still a gap in the result, and I'll point it out later.

A Warm-Up

THEOREM. α, β pos irrational, $\alpha^{-1}+\beta^{-1}=1$. Then $A:=\cup_{n=1}^{\infty} \lfloor n\alpha \rfloor$ and $B:=\cup_{n=1}^{\infty} \lfloor n\beta \rfloor$ split $\mathbb{Z}_{\geq 1}$.

Proof from the book. $\zeta=\{\alpha,\beta,2\alpha,2\beta,3\alpha,3\beta\ldots\}$. Suffices to show that precisely one term of ζ is in $[h,h+1)$ for every $h\in\mathbb{Z}_{\geq 1}$.

```
|-x----|----x-|--x---|---x--|---x--|…
1      2      3      4      5      6
```

Suffices to show that if $B\in\mathbb{Z}_{\geq 2}$, $\exists$ $N=B-1$ terms of ζ less than B.

Show: $\exists$ N=B-1 Terms of ζ Less Than B.

$n\alpha<B$ for $n=1,\ldots,\lfloor B/\alpha \rfloor$, $n\beta<B$ for $n=1,\ldots,\lfloor B/\beta \rfloor$.

Hence $N=\lfloor B/\alpha \rfloor+\lfloor B/\beta \rfloor$. Now,

$(B/\alpha)-1<\lfloor B/\alpha \rfloor<B/\alpha$, $(B/\beta)-1<\lfloor B/\beta \rfloor<B/\beta$.

Adding: $B-2<N<B$.

The 3 sides are integers and the inequalities are strict.

Hence N=B-1 as required.

Our Games are 2-Player Perfect Info; Last Player Wins

Generalized Wythoff's game played on 2 piles of tokens. Moves: either take any pos number from <u>single</u> pile or m>0 from one, n>0 from the other, provided |m-n|<a, where $a \in \mathbb{Z}_{>0}$ is a fixed integer parameter.

N-position: a position such that the <u>Next</u> (first) player can win.

P-position: a position such that the <u>Previous</u> (second) player can win.

P-positions for a=2:

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17
6	8	20

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17
6	8	20
7	9	23

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17
6	8	20
7	9	23
8	11	27

P-Positions for a=2

n	A_n	B_n
0	0	0
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17
6	8	20
7	9	23
8	11	27
9	12	30

The Rule of the Table

For S½z ¸0, S≠z ¸0, define

mex S=min z ¸0\S=least nonnegative integer not in S. Then THEOREM.

A_n=mex{A_i,B_i : 0·i<n}, B_n=A_n+2n (n ¸ 0).

This result provides a ***recursive*** strategy.

Put A=∪$_{n ¸ 1}$ A_n, B=∪$_{n ¸ 1}$ B_n. Then A, B partition z ¸1.

Is the Recursive Strategy Efficient?

Given (x,y), $0 \cdot x \cdot y$, what's the complexity of the <u>membership question</u>: Is there n such that $(x,y)=(A_n,B_n)$?

Since $B_{n+1}-B_n=A_{n+1}-A_n+2$ ¸ 3, we have $n \cdot A_n<2n$. So need to check at most 2n numbers for deciding whether $x \in A$.

Is this algorithm therefore linear?

No, it's exponential!

Is there a Polynomial Algorithm?

Let $\alpha=\sqrt{2}$, $\beta=\alpha+2$. Put $A'_n=\lfloor n\alpha \rfloor$, $B'_n=\lfloor n\beta \rfloor$.

THEOREM. $A_n=A'_n$, $B_n=B'_n$.

PROOF. Note that $A_0=A'_0=0$, $B_0=B'_0=0$. Also, $B_n-A_n=B'_n-A'_n=2n$. Moreover, A'_n, B'_n are complementary, since $\alpha^{-1}+\beta^{-1}=1$. Therefore

$$A'_n=\text{mex}\{A'_i, B'_i : 0 \le i<n\}=A_n.$$

This theorem leads to a polynomial strategy.

Another Polynomial Strategy

Continued fraction expansion of α =[1,a_1,a_2,…] (1<α<2). The numerators of the *convergents* p_n/q_n=[1,a_1,…,a_n] satisfy the recursion p_0=1, p_1=a_1+1, p_n=$a_n p_{n-1}$+p_{n-2} (n ¸ 2).

LEMMA. Every pos integer can be written uniquely in the form $N=\sum_{i=0}^{m} s_i p_i$, 0·s_i·a_{i+1}, and the special proviso $s_{i+1}=a_{i+2} \Rightarrow s_i=0$ (i ¸ 0).

Example for α=[1,2,2,2,…] on next slide.

A Polynomial Arithmetic Strategy (a=2)

7	3	1	n	A_n	B_n
			0	0	0
		1	1	1	3
		2	2	2	6
	1	0	3	4	10
	1	1	4	5	13
	1	2	5	7	17
	2	0	6	8	20
1	0	0	7	9	23
1	0	1	8	11	27
1	0	2	9	12	30
1	1	0	10	14	34
1	1	1	11	15	37
1	1	2	12	16	40

References

W.A. Wythoff, A modification of the game of Nim, Nieuw Arch. Wisk. **7** (1907) 199--202. (The case a=1, i.e., only the same number of token can be taken from both piles.)

F, How to beat your Wythoff games' opponent on three fronts, *Amer. Math. Monthly* **89** (1982) 353—36.

This ends the background material.

Apparently Complex Sequences

For $n \in \mathbb{Z}_{\geq 0}$, define the sequences

$a_n = \text{mex}\{a_i, b_i : 0 \leq i < n\}$, $b_n = a_n + \lfloor n/2 \rfloor$.

They are in Sloane's encyclopedia, but do not appear to have a succinct description.

Do the sqncs $s_n = \lfloor n\alpha \rfloor$, $t_n = \lfloor n\beta \rfloor$ approximate the above, where $\alpha = (3+\sqrt{17})/4$, $\beta = \alpha + 1/2$?

Why should they?

Note: $x^{-1} + (x+1/2)^{-1} = 1$ has the solution $x = \alpha$. Both pairs of sequences split $\mathbb{Z}_{\geq 1}$.

a_n	b_n	n	s_n	t_n
0	0	0	0	0
1	1	1	1	2
2	3	2	3	4
4	5	3	5	6
6	8	4	7	9
7	9	5	8	11
10	13	6	10	13
11	14	7	12	15
12	16	8	14	18
15	19	9	16	20
17	22	10	17	22
18	23	11	19	25

Conjectures

CONJECTURE 1. Is it the case that $a_n \cdot s_n \cdot a_n+2$ for all $n\in_{z}\;_{¸0}$?

If this holds then it's easy to show that

$b_n \cdot t_n \cdot b_n+3$ for all $n\in_{z}\;_{¸0}$.

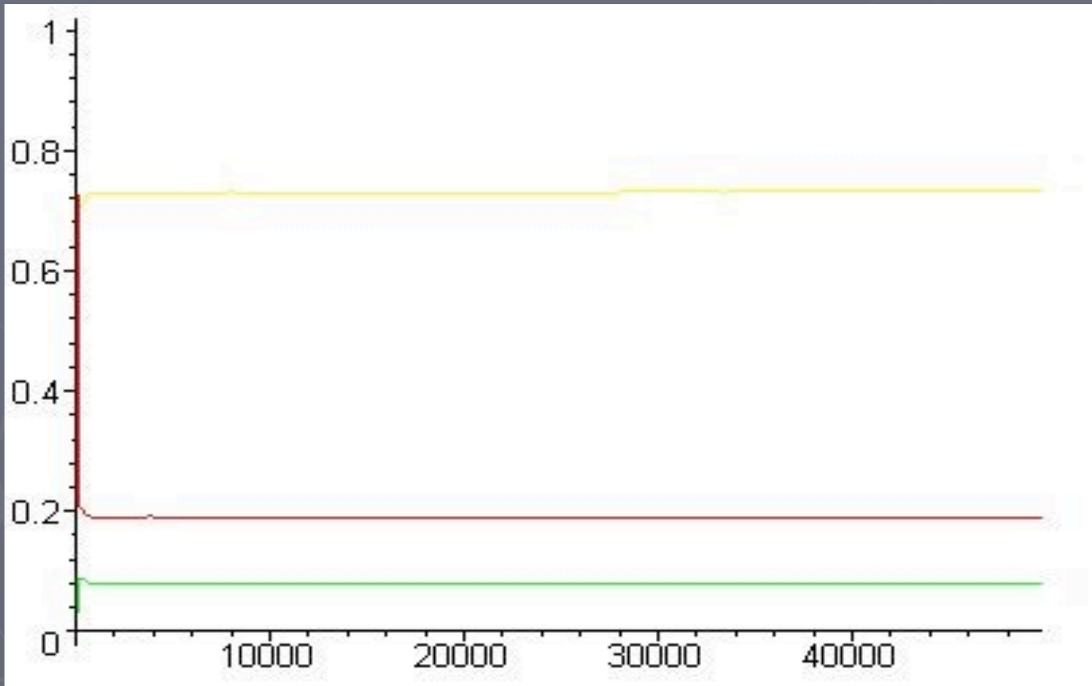
CONJECTURE 2. Is it true that for the majority of n, $a_n=s_n-1$ and $b_n=t_n-1$?

Numerical Evidence

Eric Duchene has verified Conjecture 1 for n· 100,000. %age of n for which $a_n=s_n$ is 19%, $a_n=s_n-1$: 73%, $a_n=s_n-2$: 8%. Plots follow below. They form strikingly straight lines. %age of n for which $b_n=t_n$: 9,8%, $b_n=t_n-1$: 65.4%, $b_n=t_n-2$: 24.7%, $b_n=t_n-3$: 0,02%. %ages again have very small variation when n grows. Smallest n for which $t_n=b_n+3$ is n=723.

Dorit Ron has verified Conj 1 for n·10^7 .

$a_n = s_n - 1$, $a_n = s_n$, $a_n = s_n - 2$



Conj 1 became Thm, 2 weeks ago

THEOREM 1, joint with Udi Haddad. For all $n \in$z ¸0 we have, $a_n \cdot s_n \cdot a_n+2$.

Sketch of proof.

<u>Lemma 1</u>. If $a_m \cdot 2m-2$, then

$a_n+a_m \cdot a_{n+m} \cdot a_n+a_{m+1}+1$.

<u>Cor 1.</u> $b_n+b_m \cdot b_{n+m} \cdot b_n+b_{m+1}+1$.

Auxiliary Result

For proving Lemma 1, we use

Lemma 2. There exists $c \in \mathbb{Z}$, independent of n, such that for all sufficiently large n,

$$b_{a_n - n + c} < a_n < b_{a_n - n + c + 1}$$

Fekete's Lemma

<u>Definition</u>. Sequence $\{a_n\}_{n \ge 1}$ is <u>subadditive</u> if $a_{m+n} \le a_m + a_n$ for all m, n. It's <u>superadditive</u> if $a_m + a_n \le a_{m+n}$ for all m, n.

<u>Fekete's Lemma.</u> If $\{a_n\}_{n \ge 1}$ is subadditive then lim a_n/n exists and its value is inf a_n/n (might be $-\infty$). If $\{a_n\}_{n \ge 1}$ is superadditive then lim a_n/n exists and its value is sup a_n/n (might be ∞).

Establishing the Left-Hand Inequality: $a_n \cdot s_n$

- By Fekete’s Lemma and $a_m + a_n \cdot a_{m+n}$ we have $a_n/n \rightarrow \sup a_n/n := \alpha$, $b_n/n \rightarrow \sup b_n/n := \beta$.
- $(b_n - a_n)/n \rightarrow 1/2$, so $\beta = \alpha + 1/2$.
- As in the warm-up, $\alpha^{-1} + \beta^{-1} = 1$.
- By Fekete, $\alpha = \sup a_n/n$. Hence $a_n \cdot n\alpha$, so $a_n \cdot \lfloor n\alpha \rfloor = s_n$.

Right-Hand Inequality: $s_n \le a_n+2$

From Lemma 2: $a_{n+m} \le a_n+a_{m+1}+1$. Increase n by 1: $a_{n+1+m} \le a_{n+1}+a_{m+1}+1$. Put $A_k:=a_{k+1}$. Then $A_{n+m} \le A_n+A_m+1$. Add 1: $(A_{n+m}+1) \le (A_n+1)+(A_m+1)$. Put $B_k:=A_k+1$. Then $B_{n+m} \le B_n+B_m$.

By Fekete, $B_n/n \to \inf B_n/n$. Now $B_n=A_n+1=a_{n+1}+1$, so $(a_{n+1}+1)/n \to \inf (a_{n+1}+1)/n=\alpha$. Hence $a_{n+1}+1 \ge n\alpha$. So $a_{n+1} \ge n\alpha -1=(n+1)\alpha-\alpha-1> (n+1)\alpha-3 \ge \lfloor(n+1)\alpha\rfloor-3=s_{n+1}-3$. So $s_{n+1} \le a_{n+1}+2$.

Las Vegas

- A strengthened Conj 2, namely in over 73% of n we have $a_n=s_n+1$, seems to follow from the form of the fractional part of α. Not yet done.
- So if a game with the above P-positions is put up in Las Vegas, then our probabilistic strategy will beat the house in 73% of the games..

Lemma 3

Let $U \in \mathbb{Z}_{\geq 1}$. (i) For indexes $m=m(U)$, $n=n(U)$ such that $a_m \cdot U < a_{m+1}$, $b_n \cdot U < b_{n+1}$, we have $m(U)+n(U)=U+1$.

(ii) For indexes $m'=m'(U)$, $n'=n'(U)$ such that $s_{m'} \cdot U < s_{m'+1}$, $t_{n'} \cdot U < t_{n'+1}$: $m'(U)+n'(U)=U$.

Proof of (ii). Since the s- and t-sequences split $\mathbb{Z}_{\geq 1}$, the integers in $[s_1, s_{m'}] \cup [t_1, t_{n'}]$ are but a permutation of $\{1,\ldots,U\}$. Thus $m'+n'=U$. For (i), the number 1 is assumed twice..

Corollary and Theorem

<u>COROLLARY 2.</u>

$m(U)+n(U)=m'(U)+n'(U)+1=U+1.$

Theorem 1 implies:

<u>Theorem 2.</u> For every U∈ℤ ¸1, m(U) ¸ m’(U), n(U) ¸ n’(U).

Thus Corollary 2 implies either m=m’, n=n’+1, or else m=m’+1, n=n’.

Appreciation

Thank you for listening or sleeping..

Equivalence

THEOREM 3. Theorems 1 and 2 are equivalent.

In other words, the assertion $a_n \cdot s_n \cdot a_n+2$ for all ž ¸ 1, is equivalent to m(U) ¸ m’(U), n(U) ¸ n’(U).

Proof depends on a few technical lemmas.

General Class of Games on 2 Piles

Throughout assume $x \cdot y$.

(a) Remove any pos number from *single* pile.

(b) Move $(x_0,y_0) \rightarrow (x_1,y_1)$ by removing $m>0$ from one, $n>0$ from the other pile, such that

$|m-n|=|(y_0-y_1)-(x_0-x_1)|=|(y_0-x_0)-(y_1-x_1)|<$ $f(x_1,y_1,x_0)$, f a real ***constraint function***.

Examples: (i) $f=x_1+1$; (ii) $f=x_0-x_1$.

P-Positions for $f=x_1+1$

n	0	1	2	3	4	5	6	7	8	9	10
a_n	0	1	3	4	5	7	8	9	10	12	13
b_n	0	2	6	11	17	25	34	44	55	68	82

THM. $P=\cup_{n \geq 0} (a_n, b_n)$, $a_n=\text{mex}\{a_i,b_i : 0 \leq i<n\}$,
$b_n=b_{n-1}+a_n+1$ $(b_{-1}=-1, n \geq 0)$.
Is there a polynomial strategy?

Goedel, Escher Bach Connection

Hofstaedter asks the reader in his well-known book to characterize the sequence:

B'={1,3,7,12,18,26,35,45,56,…}.

Answer: A'={2,4,5,6,8,10,11,…} is both the set of differences of consecutive terms of B', and the complement of B'.

The P-Positions and Goedel, Escher, Bach

n	0	1	2	3	4	5	6	7	8	9	10
a_n	0	1	3	4	5	7	8	9	10	12	13
b_n	0	2	6	11	17	25	34	44	55	68	82
A′	0	2	4	5	6	8	9	10	11	13	14
B′	1	3	7	12	18	26	35	45	56	69	83

P-Positions for $f = x_0 - x_1$

n	0	1	2	3	4	5	6	7	8	9	10
a_n	0	1	3	4	5	7	9	11	12	13	15
b_n	0	2	6	8	10	14	18	22	24	26	30

THM. $P = \cup_{n \ge 0} (a_n, b_n)$,

$a_n = \text{mex}\{a_i, b_i : 0 \le i < n\}$, $b_n = 2a_n$ $(n \ge 0)$.

Is there a polynomial strategy?

Yes, as indicated next:

P-Positions and Prouhet-Thue-Morse

n	0	1	2	3	4	5	6	7	8	9	10
a_n	0	1	3	4	5	7	9	11	12	13	15
b_n	0	2	6	8	10	14	18	22	24	26	30

a_n: (1) All pos integers with binary representation ending in even number of 0s. (2) Parity of number of 1's in binary representation alternates. (3) Complement is double the sequence. So b_n contains all pos integers with binary representation ending in odd number of 0s. $C_n = 0^{a_1 - a_0} 1^{a_2 - a_1} 0^{a_3 - a_2} \ldots 0^{a_{2n+1} - a_{2n}} 1^{a_{2n+2} - a_{2n+1}}$. $= 011010011001011010010\ldots$ is the famous PTM sequence.

Master Theorem

THEOREM. $S=\cup_{i \geq 0} (a_i,b_i)$, $a_n=\text{mex}\{a_i,b_i : 0 \leq i<n\}$,

$b_n=f(a_{n-1},b_{n-1}, a_n)+b_{n-1}+a_n-a_{n-1}$.

If f is positive, monotone and semi-additive, then S is the set of P-positions of a general 2-pile subtraction game with constraint function f.

Epilogue

For any given infinite binary word W, put A={locations of 0s}, B={locations of 1s}. Then (A,B) constitute the P-positions of some game G. If the subword complexity of W is sufficiently high, the membership question for (A,B) likely doesn't have a polynomial solution. Then look for an approximating sequence.