# Differential addition chains

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
Danmarks Tekniske Universitet
Alfred P. Sloan Foundation

Motivating problem:
Given elliptic curve $E$,
integer $n$, and point $P$ on $E$,
compute $nP$ on $E$
as quickly as possible.

Many variations of problem.
Some applications reuse one $n$
for many $P$'s.
Some applications don't.
Some applications use secret $n$;
must not leak $n$ through timing.
Some applications use public $n$.
Etc.

ion chains

ois at Chicago
ske Universitet
Foundation

Motivating problem:
Given elliptic curve $E$,
integer $n$, and point $P$ on $E$,
compute $nP$ on $E$
as quickly as possible.

Many variations of problem.
Some applications reuse one $n$
for many $P$'s.
Some applications don't.
Some applications use secret $n$;
must not leak $n$ through timing.
Some applications use public $n$.
Etc.

1987 Montgomer

Focus on large-ch
curves $y^2 = x^3 +$
with small $a \in \{$

Use pair $(x, z)$ to
$P = (x/z, \ldots)$.

Computing $Q$, $R$,
takes 6 mults.
Only 5 mults if $Q$
denominator.
Only 4 mults if $Q$
numerator and sn
Only 4 mults if $Q$

Motivating problem:
Given elliptic curve $E$,
integer $n$, and point $P$ on $E$,
compute $nP$ on $E$
as quickly as possible.

Many variations of problem.
Some applications reuse one $n$
for many $P$'s.
Some applications don't.
Some applications use secret $n$;
must not leak $n$ through timing.
Some applications use public $n$.
Etc.

1987 Montgomery:

Focus on large-characteristic
curves $y^2 = x^3 + ax^2 + x$
with small $a \in \{6, 10, 14, \ldots\}$.

Use pair $(x, z)$ to represent point
$P = (x/z, \ldots)$.

Computing $Q, R, Q - R \mapsto Q + R$
takes 6 mults.
Only 5 mults if $Q - R$ has small
denominator.
Only 4 mults if $Q - R$ has small
numerator and small denominator.
Only 4 mults if $Q = R$.

em:

ve $E$,

oint $P$ on $E$,

$E$

sible.

of problem.

ns reuse one $n$

ns don't.

ns use secret $n$;

through timing.

ns use public $n$.

1987 Montgomery:

Focus on large-characteristic curves $y^2 = x^3 + ax^2 + x$ with small $a \in \{6, 10, 14, \ldots\}$.

Use pair $(x, z)$ to represent point $P = (x/z, \ldots)$.

Computing $Q, R, Q - R \mapsto Q + R$ takes 6 mults.
Only 5 mults if $Q - R$ has small denominator.
Only 4 mults if $Q - R$ has small numerator and small denominator.
Only 4 mults if $Q = R$.

Given $n$, write $P$

as composition o

$Q, R, Q - R \mapsto Q$

e.g. $n = 10$: cor

$P, \; P, \; 0 \mapsto 2P$

$2P, \; P, P \mapsto 3P$

$3P, 2P, P \mapsto 5P$

$5P, 5P, \; 0 \mapsto 10P$

Overall 20 mults

Only 18 mults

if $P$ has small de

Only 16 mults

if $P$ has small nu

small denominato

1987 Montgomery:

Focus on large-characteristic curves $y^2 = x^3 + ax^2 + x$ with small $a \in \{6, 10, 14, \ldots\}$.

Use pair $(x, z)$ to represent point $P = (x/z, \ldots)$.

Computing $Q, R, Q - R \mapsto Q + R$ takes 6 mults.
Only 5 mults if $Q - R$ has small denominator.
Only 4 mults if $Q - R$ has small numerator and small denominator.
Only 4 mults if $Q = R$.

Given $n$, write $P \mapsto nP$ as composition of additions $Q, R, Q - R \mapsto Q + R$.

e.g. $n = 10$: compute
$P, \; P, \; 0 \mapsto 2P$ with 4 mults;
$2P, \; P, P \mapsto 3P$ with 6 mults;
$3P, 2P, P \mapsto 5P$ with 6 mults;
$5P, 5P, \; 0 \mapsto 10P$ with 4 mults.
Overall 20 mults for $P \mapsto 10P$.
Only 18 mults if $P$ has small denominator.
Only 16 mults if $P$ has small numerator and small denominator.

ry:

haracteristic

$- ax^2 + x$

$6, 10, 14, \ldots\}$.

o represent point

$, Q - R \mapsto Q + R$

$Q - R$ has small

$Q - R$ has small
mall denominator.
$Q = R$.

Given $n$, write $P \mapsto nP$
as composition of additions
$Q, R, Q - R \mapsto Q + R$.

e.g. $n = 10$: compute
$P, \ P, \ 0 \mapsto 2P$ with 4 mults;
$2P, \ P, P \mapsto 3P$ with 6 mults;
$3P, 2P, P \mapsto 5P$ with 6 mults;
$5P, 5P, \ 0 \mapsto 10P$ with 4 mults.
Overall 20 mults for $P \mapsto 10P$.
Only 18 mults
if $P$ has small denominator.
Only 16 mults
if $P$ has small numerator and
small denominator.

$0, P, 2P, 3P, 5P, 1$
**differential addi**
starting from 0, $P$
each subsequent
is $Q + R$ for som
$Q, R, Q - R$ alre

0, 1, 2, 3, 5, 10 is
differential additi
starting from 0, 1

Question: Given
short differential
starting from 0, 1
Variations: meas
by mults, CPU c

Given $n$, write $P \mapsto nP$ as composition of additions $Q, R, Q-R \mapsto Q+R$.

e.g. $n = 10$: compute
$P, \ P, \ 0 \mapsto 2P$ with 4 mults;
$2P, \ P, P \mapsto 3P$ with 6 mults;
$3P, 2P, P \mapsto 5P$ with 6 mults;
$5P, 5P, \ 0 \mapsto 10P$ with 4 mults.
Overall 20 mults for $P \mapsto 10P$.
Only 18 mults if $P$ has small denominator.
Only 16 mults if $P$ has small numerator and small denominator.

$0, P, 2P, 3P, 5P, 10P$ is a **differential addition chain** starting from $0, P$: each subsequent term is $Q+R$ for some $Q, R, Q-R$ already in chain.

$0, 1, 2, 3, 5, 10$ is a differential addition chain starting from $0, 1$.

Question: Given $n$, how to find short differential addition chain starting from $0, 1$ and ending $n$? Variations: measure shortness by mults, CPU cycles, etc.

$P \mapsto nP$
f additions
$Q + R$.

mpute
with 4 mults;
with 6 mults;
with 6 mults;
$P$ with 4 mults.
for $P \mapsto 10P$.

enominator.

umerator and
or.

$0, P, 2P, 3P, 5P, 10P$ is a
**differential addition chain**
starting from $0, P$:
each subsequent term
is $Q + R$ for some
$Q, R, Q - R$ already in chain.

$0, 1, 2, 3, 5, 10$ is a
differential addition chain
starting from $0, 1$.

Question: Given $n$, how to find
short differential addition chain
starting from $0, 1$ and ending $n$?
Variations: measure shortness
by mults, CPU cycles, etc.

The binary meth
obtain $n, n + 1$ f
$\lfloor n/2 \rfloor, \lfloor n/2 \rfloor +$
one addition wit
one addition wit

e.g.
$13P, 13P, 0 \mapsto 2$
$14P, 13P, P \mapsto 2$
if $P$ has small de

Overall 9 mults
for each bit of $n$
if $P$ has small de

$0, P, 2P, 3P, 5P, 10P$ is a **differential addition chain** starting from $0, P$: each subsequent term is $Q + R$ for some $Q, R, Q - R$ already in chain.

$0, 1, 2, 3, 5, 10$ is a differential addition chain starting from $0, 1$.

Question: Given $n$, how to find short differential addition chain starting from $0, 1$ and ending $n$? Variations: measure shortness by mults, CPU cycles, etc.

The binary method: obtain $n, n + 1$ from $\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1$ using one addition with difference 1, one addition with difference 0.

e.g. $13P, 13P, 0 \mapsto 26P$ with 4 mults; $14P, 13P, P \mapsto 27P$ with 5 mults, if $P$ has small denominator.

Overall 9 mults for each bit of $n$, if $P$ has small denominator.

10$P$ is a
**ition chain**
$P$:
term
ne
ady in chain.

a
on chain
..

$n$, how to find
addition chain
and ending $n$?
ure shortness
ycles, etc.

The binary method:
obtain $n, n + 1$ from
$\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1$ using
one addition with difference 1,
one addition with difference 0.

e.g.
$13P, 13P, 0 \mapsto 26P$ with 4 mults;
$14P, 13P, P \mapsto 27P$ with 5 mults,
if $P$ has small denominator.

Overall 9 mults
for each bit of $n$,
if $P$ has small denominator.

1992 Montgomer
1996 Bleichenba
2001 Tsuruoka:

Experiments for
find length $\approx 1.5$
instead of 2 per
Lower bound $\approx 1$

Count mults inst
$\approx 8.885$ per bit,
instead of 9 per

Disadvantages: h
no uniform struc
avoid leaking $n$ t

The binary method:
obtain $n, n+1$ from
$\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1$ using
one addition with difference 1,
one addition with difference 0.

e.g.
$13P, 13P, 0 \mapsto 26P$ with 4 mults;
$14P, 13P, P \mapsto 27P$ with 5 mults,
if $P$ has small denominator.

Overall 9 mults
for each bit of $n$,
if $P$ has small denominator.

1992 Montgomery,
1996 Bleichenbacher,
2001 Tsuruoka: Can do better!

Experiments for average 128-bit $n$
find length $\approx 1.533$ per bit,
instead of 2 per bit.
Lower bound $\approx 1.440$ per bit.

Count mults instead of length:
$\approx 8.885$ per bit,
instead of 9 per bit.

Disadvantages: harder to find;
no uniform structure; harder to
avoid leaking $n$ through timing.

od:
from
1 using
n difference 1,
n difference 0.

6$P$ with 4 mults;
27$P$ with 5 mults,
enominator.

,
enominator.

1992 Montgomery,
1996 Bleichenbacher,
2001 Tsuruoka: Can do better!

Experiments for average 128-bit $n$ find length $\approx 1.533$ per bit, instead of 2 per bit.
Lower bound $\approx 1.440$ per bit.

Count mults instead of length: $\approx 8.885$ per bit, instead of 9 per bit.

Disadvantages: harder to find; no uniform structure; harder to avoid leaking $n$ through timing.

Two-dimensional
Given $m, n$, how
short differential
starting from the
$(0, 0), (1, 0), (0, 1$
and ending $(m, n$

Motivating probl
Given elliptic cur
integers $m, n$,
and points $P, Q$,
compute $mP + n$
as quickly as pos

1992 Montgomery,
1996 Bleichenbacher,
2001 Tsuruoka: Can do better!

Experiments for average 128-bit $n$ find length $\approx 1.533$ per bit, instead of 2 per bit.
Lower bound $\approx 1.440$ per bit.

Count mults instead of length: $\approx 8.885$ per bit, instead of 9 per bit.

Disadvantages: harder to find; no uniform structure; harder to avoid leaking $n$ through timing.

Two-dimensional question:
Given $m, n$, how to find short differential addition chain starting from the vectors $(0,0), (1,0), (0,1), (1,-1)$ and ending $(m, n)$?

Motivating problem:
Given elliptic curve $E$, integers $m, n$, and points $P, Q, P - Q$, compute $mP + nQ$ on $E$ as quickly as possible.

ry,
cher,
Can do better!

average 128-bit $n$
533 per bit,
bit.
1.440 per bit.

ead of length:

bit.

harder to find;
ture; harder to
through timing.

Two-dimensional question:
Given $m, n$, how to find
short differential addition chain
starting from the vectors
$(0,0), (1,0), (0,1), (1,-1)$
and ending $(m, n)$?

Motivating problem:
Given elliptic curve $E$,
integers $m, n$,
and points $P, Q, P-Q$,
compute $mP + nQ$ on $E$
as quickly as possible.

For average 128-
small $P, Q, P-Q$

| dim | method |
|---|---|
| 2 | easy binary |
| 2 | Schoenmake |
| 2 | Akishita |
| 2 | new binary |
| 2 | Montgomer |
| 2 | new ext gcd |
| 1 | easy binary |
| 1 | standard |
| | Fibonacci c |

Two-dimensional question:
Given $m, n$, how to find
short differential addition chain
starting from the vectors
$(0,0), (1,0), (0,1), (1,-1)$
and ending $(m, n)$?

Motivating problem:
Given elliptic curve $E$,
integers $m, n$,
and points $P, Q, P-Q$,
compute $mP + nQ$ on $E$
as quickly as possible.

For average 128-bit exponents,
small $P, Q, P-Q$ denominators:

| dim | method | mults per bit | unif |
|---|---|---|---|
| 2 | easy binary | 19.000 | yes |
| 2 | Schoenmakers | 17.250 | no |
| 2 | Akishita | 14.250 | no |
| 2 | new binary | 14.000 | yes |
| 2 | Montgomery | 10.261 | no |
| 2 | new ext gcd | 9.918 | no |
| 1 | easy binary | 9.000 | yes |
| 1 | standard | 8.885 | no |
| | Fibonacci case | 8.643 | |

question:
to find
addition chain
e vectors
), $(1, -1)$
$n)$?

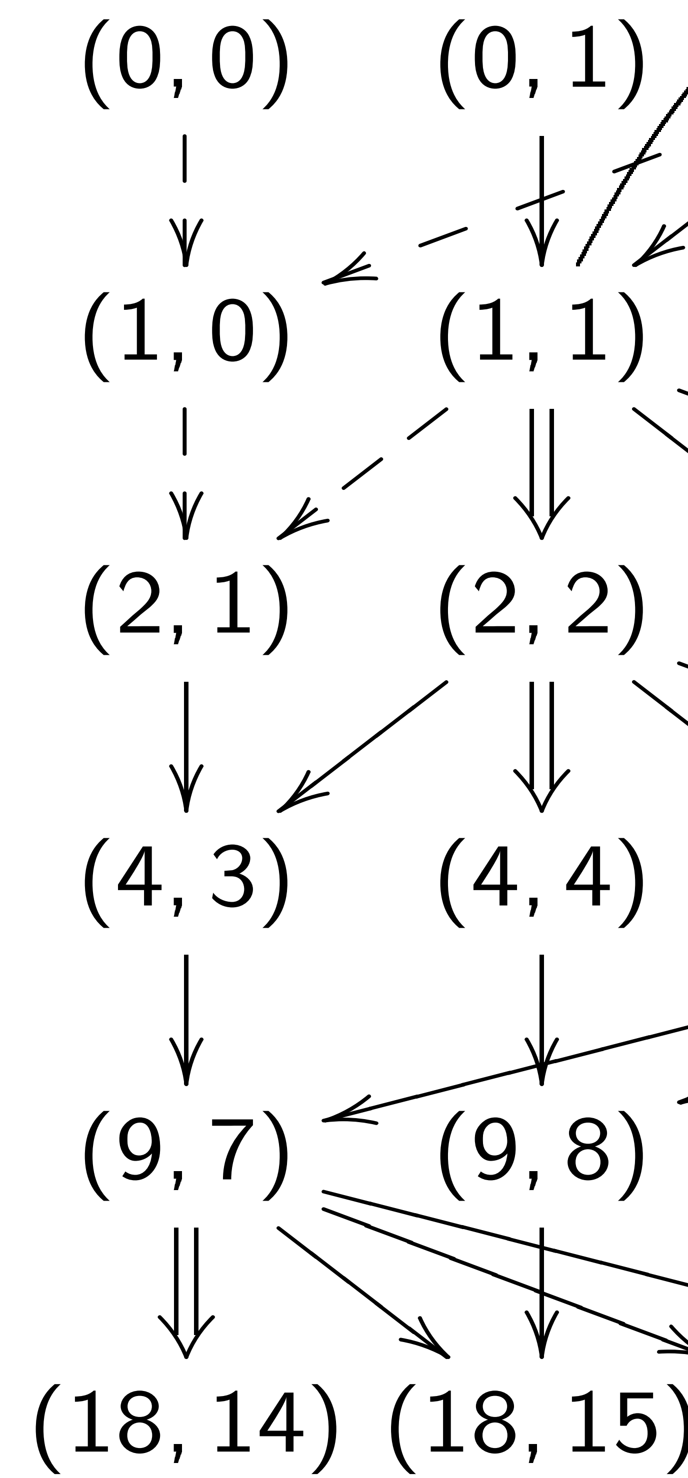
em:
ve $E$,

$P - Q$,
$nQ$ on $E$
sible.

For average 128-bit exponents, small $P, Q$, $P - Q$ denominators:

| dim | method | mults per bit | unif |
|---|---|---|---|
| 2 | easy binary | 19.000 | yes |
| 2 | Schoenmakers | 17.250 | no |
| 2 | Akishita | 14.250 | no |
| 2 | new binary | 14.000 | yes |
| 2 | Montgomery | 10.261 | no |
| 2 | new ext gcd | 9.918 | no |
| 1 | easy binary | 9.000 | yes |
| 1 | standard | 8.885 | no |
| | Fibonacci case | 8.643 | |

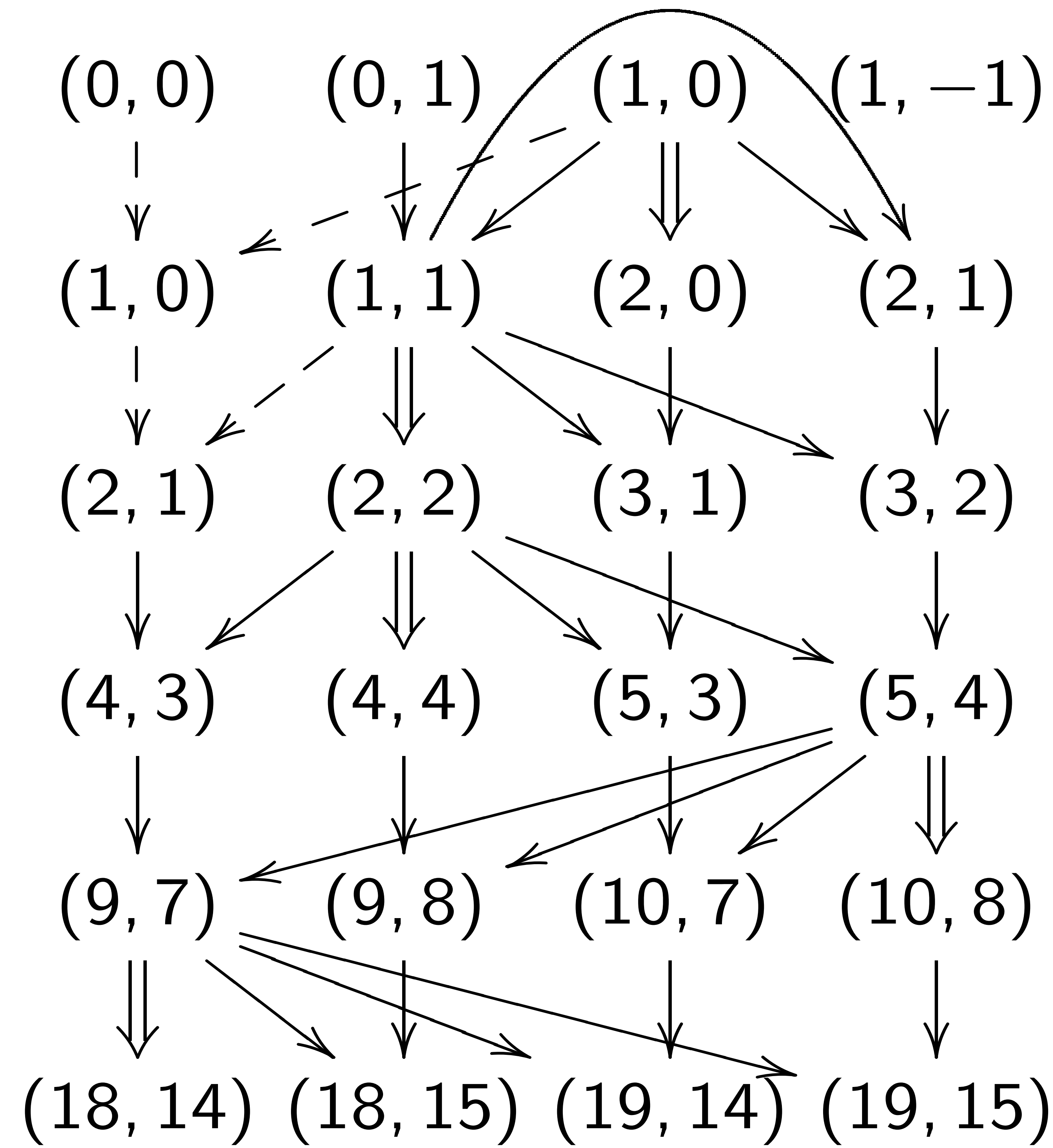
Easy dim-2 binar



For average 128-bit exponents, small $P, Q, P-Q$ denominators:

| dim | method | mults per bit | unif |
|---|---|---|---|
| 2 | easy binary | 19.000 | yes |
| 2 | Schoenmakers | 17.250 | no |
| 2 | Akishita | 14.250 | no |
| 2 | new binary | 14.000 | yes |
| 2 | Montgomery | 10.261 | no |
| 2 | new ext gcd | 9.918 | no |
| 1 | easy binary | 9.000 | yes |
| 1 | standard | 8.885 | no |
| | Fibonacci case | 8.643 | |

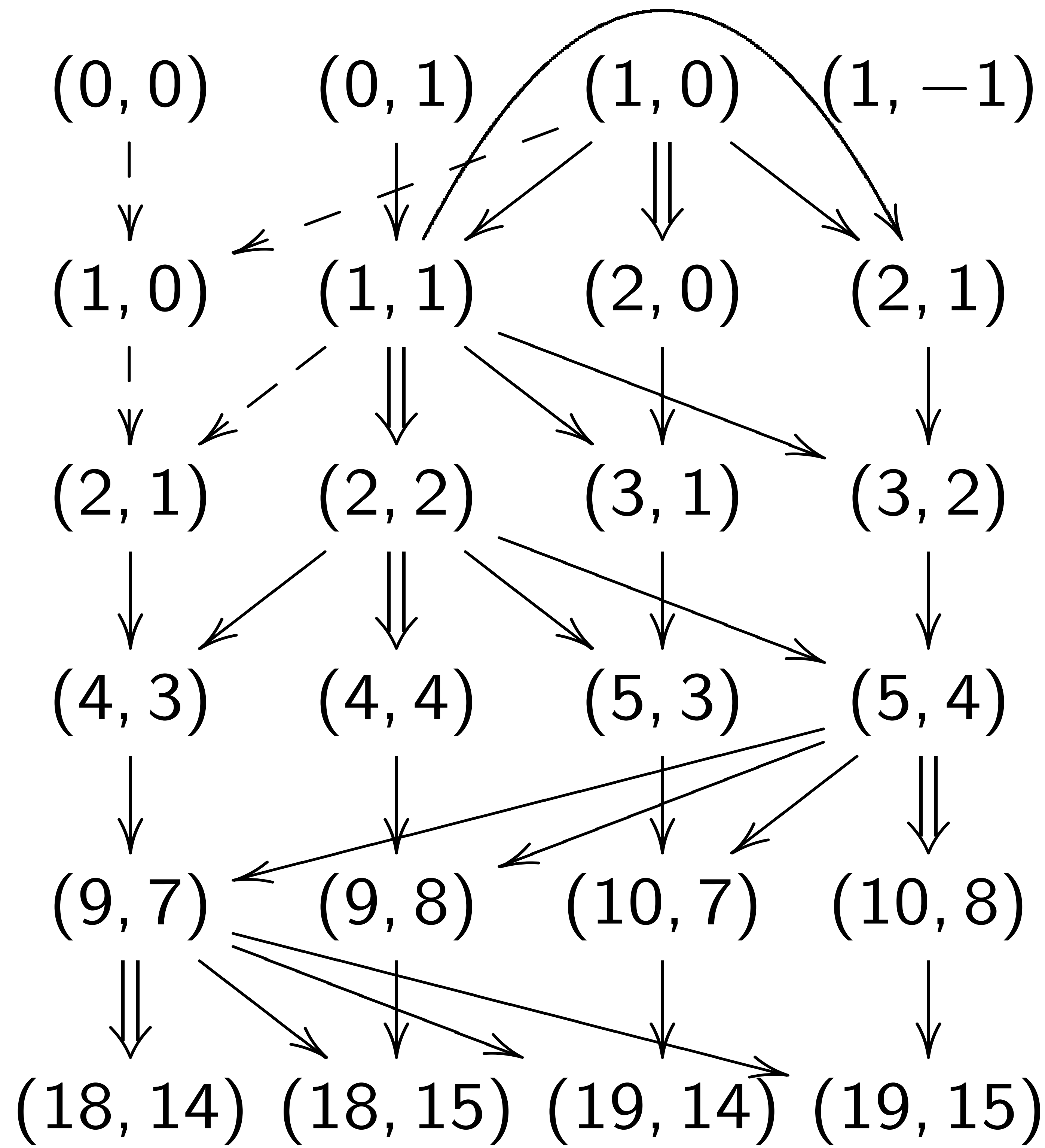
Easy dim-2 binary chain:



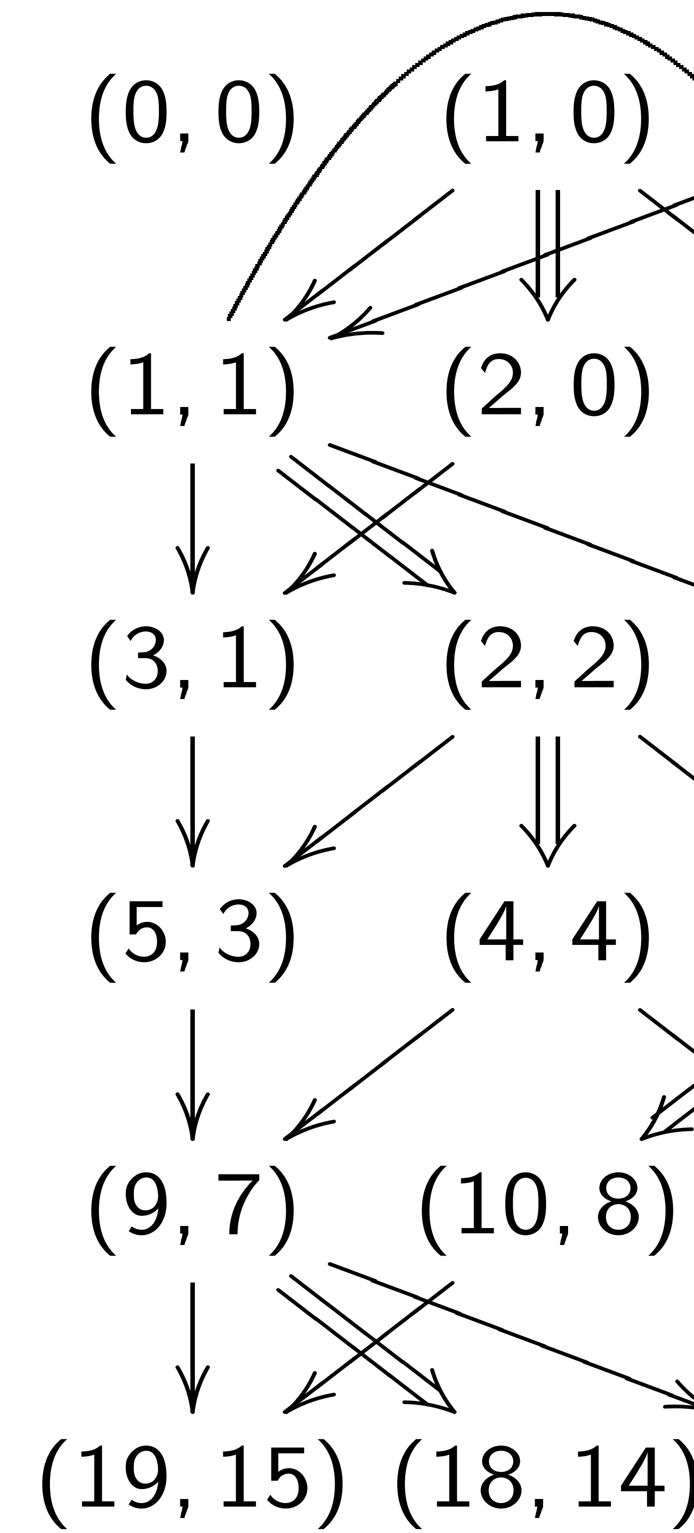
bit exponents,
Q denominators:

| | mults per bit | unif |
|---|---|---|
| | 19.000 | yes |
| ers | 17.250 | no |
| | 14.250 | no |
| | 14.000 | yes |
| y | 10.261 | no |
| d | 9.918 | no |
| | 9.000 | yes |
| | 8.885 | no |
| ase | 8.643 | |

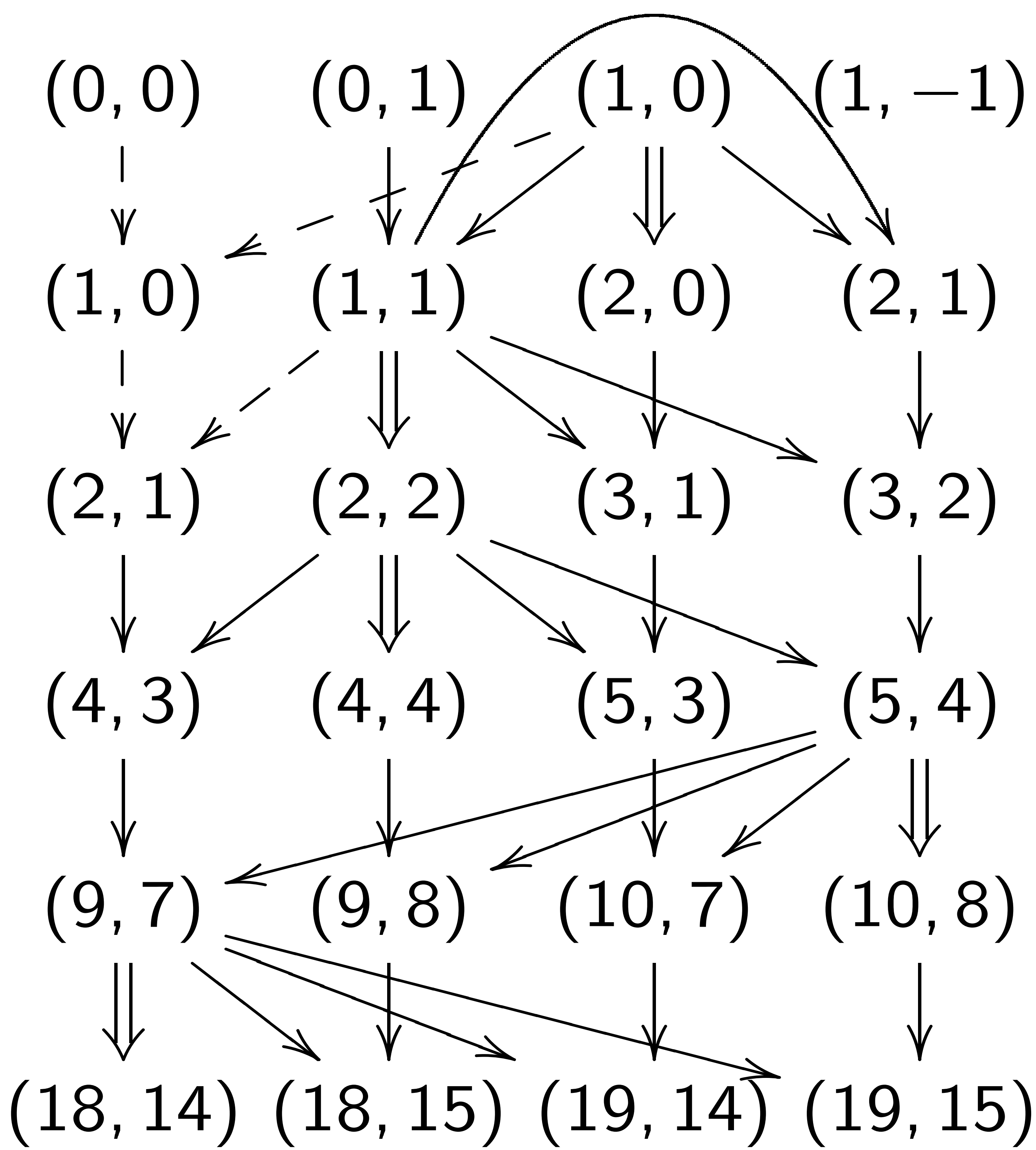
Easy dim-2 binary chain:



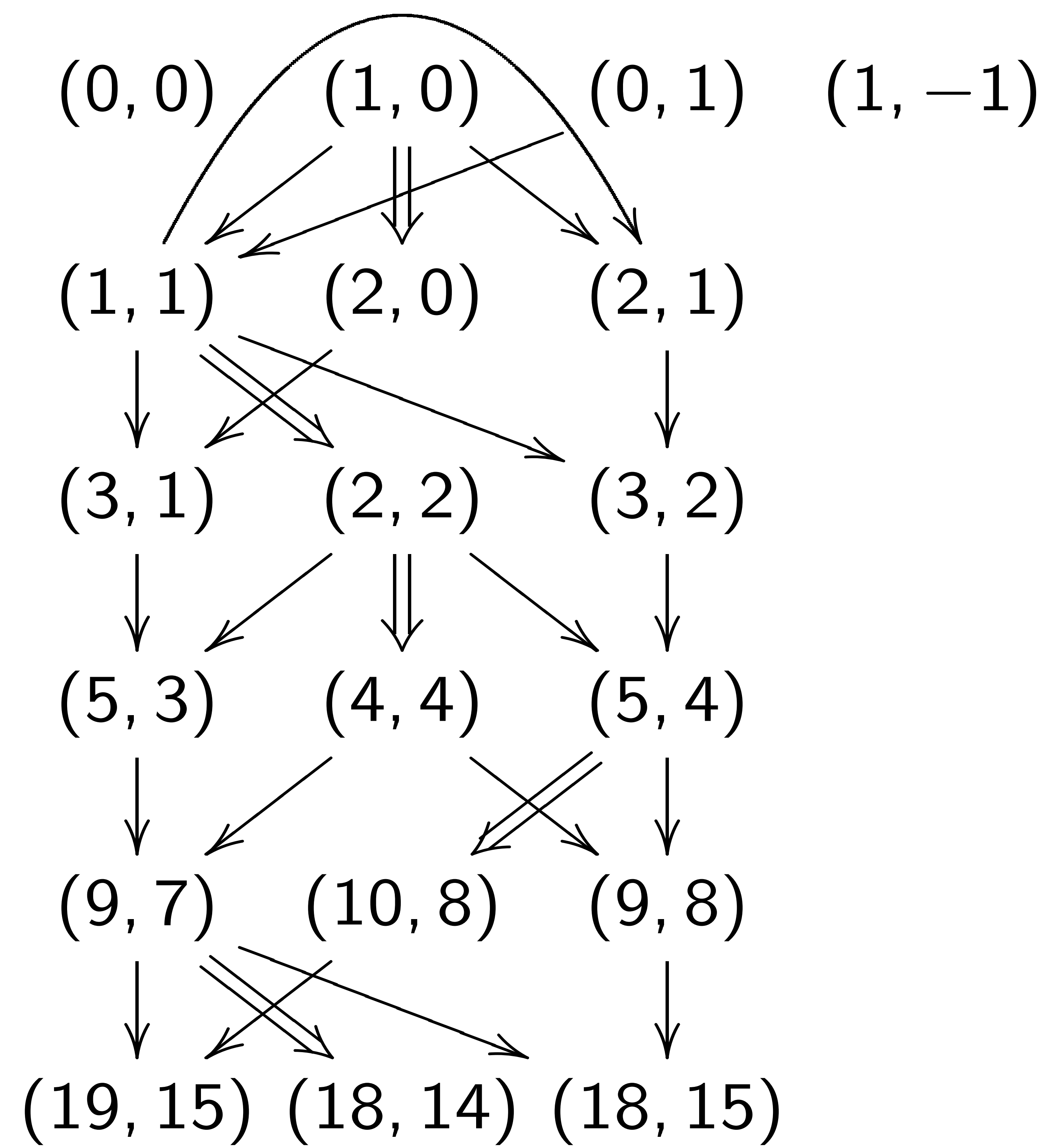

New dim-2 binar



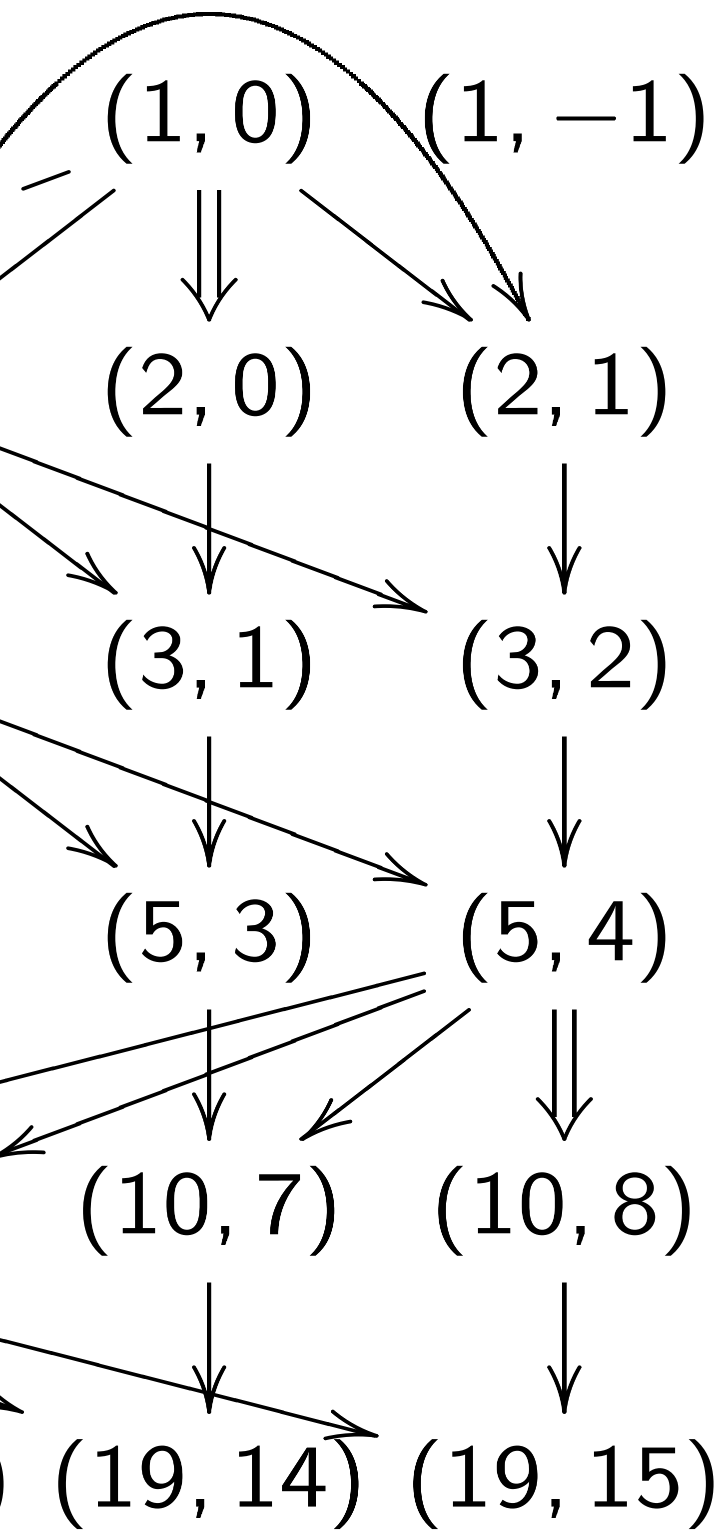
Easy dim-2 binary chain:



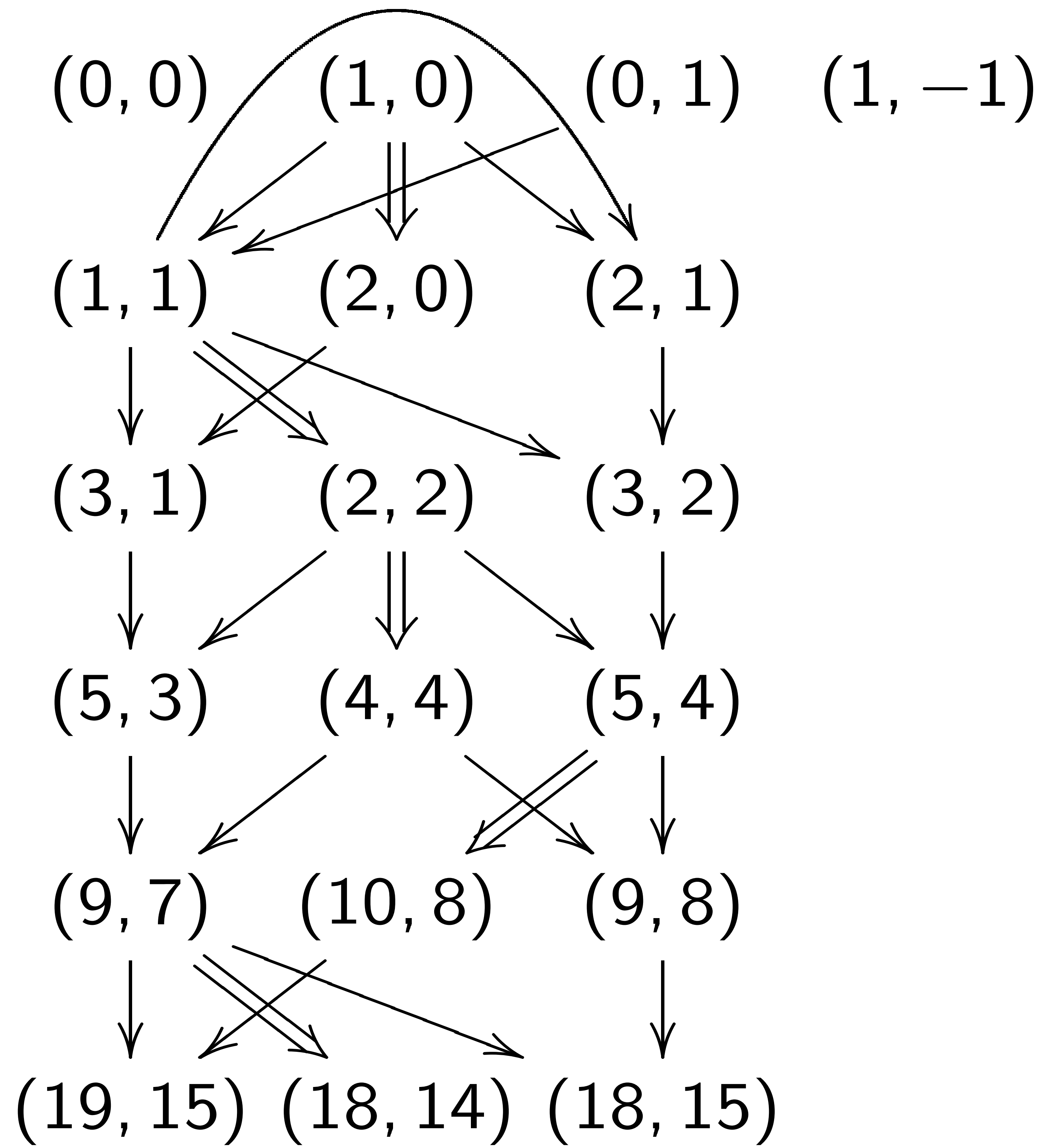

New dim-2 binary chain:



y chain:




New dim-2 binary chain:

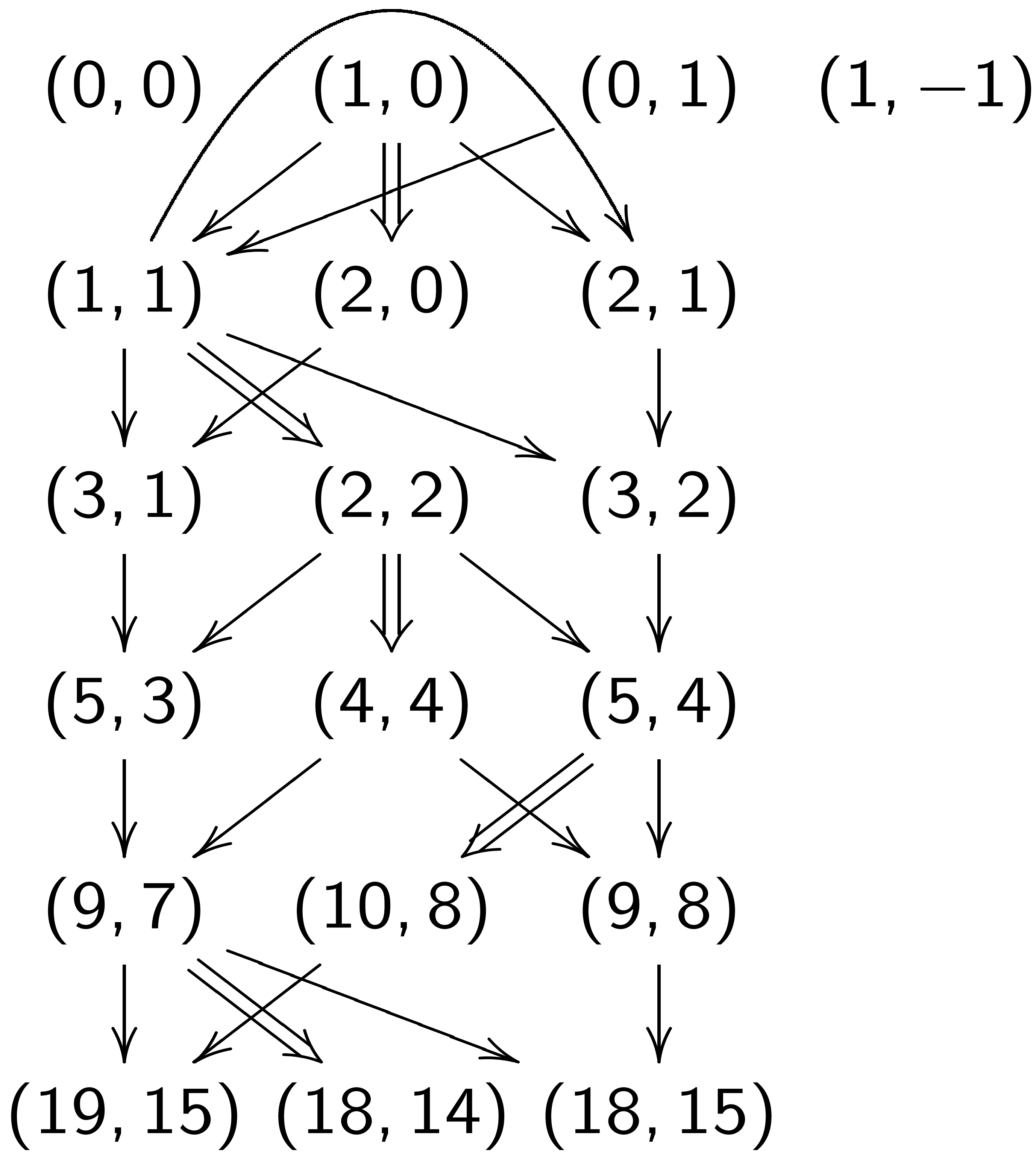



Line in easy bina
has $(a, b)$, $(a, b +$
$(a + 1, b + 1)$. O
by double-add-ac

New observation
(even, odd) or (o
chosen recursivel
next line can be
by double-add-ac
14 mults if $P, Q,$
have small denor

Intermediate resu
Schoenmakers, 2

New dim-2 binary chain:

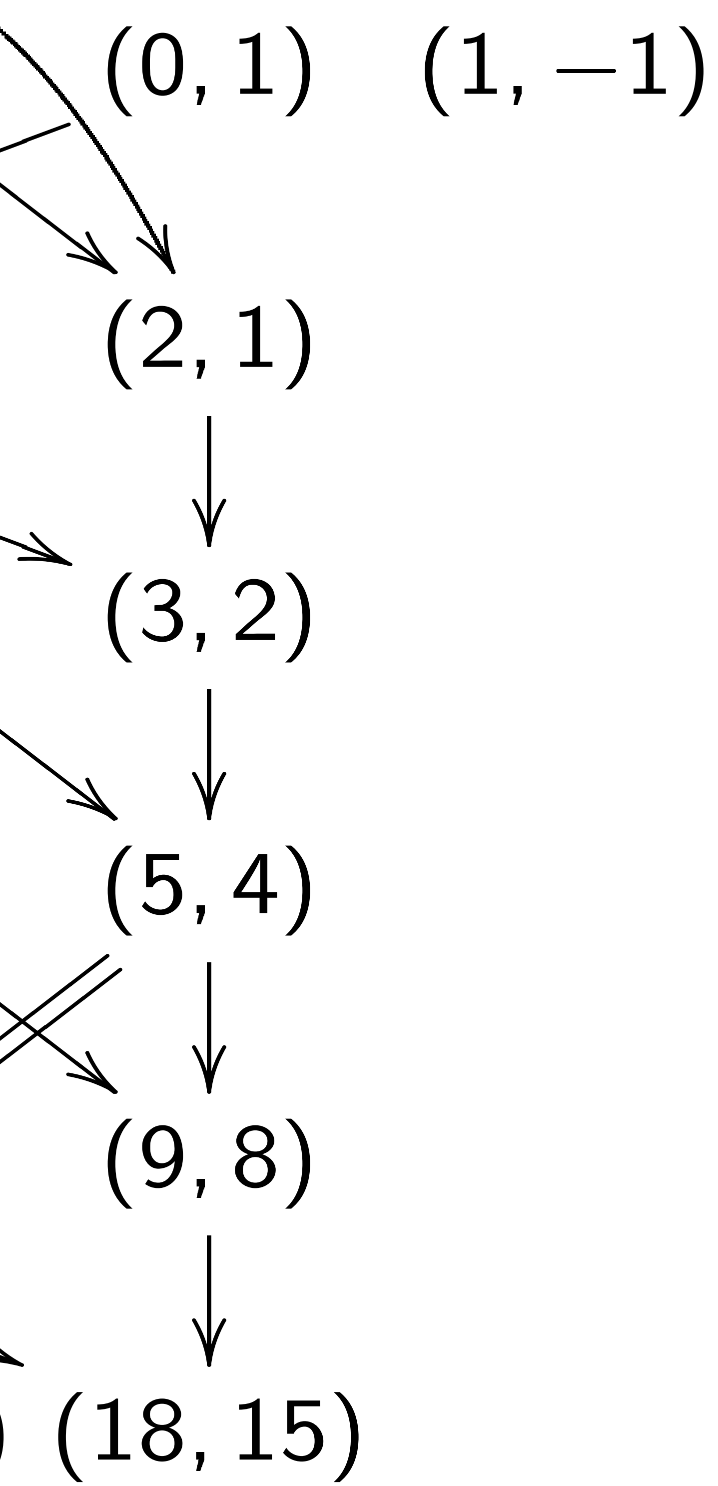



Line in easy binary chain has $(a, b)$, $(a, b+1)$, $(a+1, b)$, $(a+1, b+1)$. Obtain next line by double-add-add-add.

New observation: can omit (even, odd) or (odd, even), chosen recursively so that next line can be obtained by double-add-add. 14 mults if $P, Q, P-Q$ have small denominators.

Intermediate results: 2000 Schoenmakers, 2001 Akishita.

y chain:




Line in easy binary chain has $(a, b)$, $(a, b+1)$, $(a+1, b)$, $(a+1, b+1)$. Obtain next line by double-add-add-add.

New observation: can omit (even, odd) or (odd, even), chosen recursively so that next line can be obtained by double-add-add.
14 mults if $P, Q, P-Q$ have small denominators.

Intermediate results: 2000 Schoenmakers, 2001 Akishita.

How to do better

Don't worry abou

Critical idea for c

Build chain $0, 1,$

by choosing $r \approx$

and building chai

$0, 1, \ldots, r, n-r,$

Try many $r$'s, ke

Some further cho

could build $\{r, n$

from $\{r, n-2r,$

from $\{n-r, 2r$

from $\{r, n/2-r$

Line in easy binary chain has $(a, b)$, $(a, b + 1)$, $(a + 1, b)$, $(a + 1, b + 1)$. Obtain next line by double-add-add-add.

New observation: can omit $(\text{even}, \text{odd})$ or $(\text{odd}, \text{even})$, chosen recursively so that next line can be obtained by double-add-add. 14 mults if $P, Q, P - Q$ have small denominators.

Intermediate results: 2000 Schoenmakers, 2001 Akishita.

How to do better than binary? Don't worry about uniformity.

Critical idea for dim 1: Build chain $0, 1, \ldots, n$ by choosing $r \approx n(\sqrt{5} - 1)/2$ and building chain $0, 1, \ldots, r, n - r, n$. Try many $r$'s, keep best.

Some further choices here: could build $\{r, n - r, n\}$ from $\{r, n - 2r, n - r\}$ or from $\{n - r, 2r - n, r\}$ or from $\{r, n/2 - r, n/2\}$ or $\ldots$.

ry chain
+ 1), $(a + 1, b)$,
Obtain next line
dd-add.

: can omit
dd, even),
y so that
obtained
dd.
$P - Q$
minators.

ults: 2000
001 Akishita.

How to do better than binary?
Don't worry about uniformity.

Critical idea for dim 1:
Build chain $0, 1, \ldots, n$
by choosing $r \approx n(\sqrt{5} - 1)/2$
and building chain
$0, 1, \ldots, r, n - r, n$.
Try many $r$'s, keep best.

Some further choices here:
could build $\{r, n - r, n\}$
from $\{r, n - 2r, n - r\}$ or
from $\{n - r, 2r - n, r\}$ or
from $\{r, n/2 - r, n/2\}$ or $\ldots$.

e.g. $n = 100$, $r =$
Build chain
$0, 1, 2, 3, 5, 7, 12,$
by building $\{39, 6$
from $\{22, 39, 61\}$

What about dim
Obvious adaptati
Build chain $\ldots, ($
by choosing $(q, r$
and building chai
$\ldots, (q, r), (m -$

How to do better than binary?
Don't worry about uniformity.

Critical idea for dim 1:
Build chain $0, 1, \ldots, n$
by choosing $r \approx n(\sqrt{5} - 1)/2$
and building chain
$0, 1, \ldots, r, n - r, n$.
Try many $r$'s, keep best.

Some further choices here:
could build $\{r, n - r, n\}$
from $\{r, n - 2r, n - r\}$ or
from $\{n - r, 2r - n, r\}$ or
from $\{r, n/2 - r, n/2\}$ or ....

e.g. $n = 100$, $r = 39$:
Build chain
$0, 1, 2, 3, 5, 7, 12, 17, 22, 39, 61, 100$
by building $\{39, 61, 100\}$
from $\{22, 39, 61\}$ etc.

What about dim 2?
Obvious adaptation of idea:
Build chain $\ldots, (m, n)$
by choosing $(q, r)$
and building chain
$\ldots, (q, r), (m - q, n - r), (m, n)$.

r than binary?
ut uniformity.

dim 1:
$\ldots, n$
$n(\sqrt{5}-1)/2$
in
$, n$.
ep best.

oices here:
$-r, n\}$
$n-r\}$ or
$-n, r\}$ or
$, n/2\}$ or ....

e.g. $n = 100$, $r = 39$:
Build chain
$0, 1, 2, 3, 5, 7, 12, 17, 22, 39, 61, 100$
by building $\{39, 61, 100\}$
from $\{22, 39, 61\}$ etc.

What about dim 2?
Obvious adaptation of idea:
Build chain $\ldots, (m, n)$
by choosing $(q, r)$
and building chain
$\ldots, (q, r), (m-q, n-r), (m, n)$.

e.g. Work backw
$(314, 271)$ and (1
$(120, 104)$, then
$(46, 41)$, then (28
$(18, 19)$, then (10
$(8, 16)$.

Hmmm, what's t
How to build sho
$\{(8, 16), (10, 3),$ (

Several plausible
but all of them s
Normally this con
is abandoned.

e.g. $n = 100$, $r = 39$:
Build chain
$0, 1, 2, 3, 5, 7, 12, 17, 22, 39, 61, 100$
by building $\{39, 61, 100\}$
from $\{22, 39, 61\}$ etc.

What about dim 2?
Obvious adaptation of idea:
Build chain $\ldots, (m, n)$
by choosing $(q, r)$
and building chain
$\ldots, (q, r), (m - q, n - r), (m, n)$.

e.g. Work backwards from
$(314, 271)$ and $(194, 167)$ to
$(120, 104)$, then $(74, 63)$, then
$(46, 41)$, then $(28, 22)$, then
$(18, 19)$, then $(10, 3)$, then
$(8, 16)$.

Hmmm, what's the endgame?
How to build short chain with
$\{(8, 16), (10, 3), (18, 19)\}$?

Several plausible approaches,
but all of them scale badly.
Normally this construction
is abandoned.

= 39:

17, 22, 39, 61, 100

61, 100}

etc.

2?

ion of idea:

$(m, n)$

)

in

$q, n - r), (m, n)$.

e.g. Work backwards from (314, 271) and (194, 167) to (120, 104), then (74, 63), then (46, 41), then (28, 22), then (18, 19), then (10, 3), then (8, 16).

Hmmm, what's the endgame? How to build short chain with $\{(8, 16), (10, 3), (18, 19)\}$?

Several plausible approaches, but all of them scale badly. Normally this construction is abandoned.

New observation

Simple endgames

if $rm - qn = \Delta$

with, e.g., $\Delta =$

Often find very g

Easy to find $(q, r$

given $(m, n, \Delta)$:

standard ext-gcd

What if $(m, n)$ n

Great! Exploit fa

Try many good c

for $(\Delta, q, r)$, kee

e.g. Work backwards from $(314, 271)$ and $(194, 167)$ to $(120, 104)$, then $(74, 63)$, then $(46, 41)$, then $(28, 22)$, then $(18, 19)$, then $(10, 3)$, then $(8, 16)$.

Hmmm, what's the endgame? How to build short chain with $\{(8, 16), (10, 3), (18, 19)\}$?

Several plausible approaches, but all of them scale badly. Normally this construction is abandoned.

New observation: Simple endgames work well if $rm - qn = \Delta$ with, e.g., $\Delta = \pm 2^a 3^b$. Often find very good chains.

Easy to find $(q, r)$ given $(m, n, \Delta)$: standard ext-gcd computation.

What if $(m, n)$ not coprime? Great! Exploit factor.

Try many good choices for $(\Delta, q, r)$, keep best.

vards from
$194, 167)$ to
$(74, 63)$, then
$8, 22)$, then
$0, 3)$, then

the endgame?
ort chain with
$(18, 19)\}$?

approaches,
cale badly.
nstruction

New observation:
Simple endgames work well
if $rm - qn = \Delta$
with, e.g., $\Delta = \pm 2^a 3^b$.
Often find very good chains.

Easy to find $(q, r)$
given $(m, n, \Delta)$:
standard ext-gcd computation.

What if $(m, n)$ not coprime?
Great! Exploit factor.

Try many good choices
for $(\Delta, q, r)$, keep best.

Example of new
$(0, 0)$, $(1, 0)$, $(0,$
$(1, 1)$, $(1, 2)$, $(2,$
$(4, 7)$, $(5, 9)$, $(9,$
$(19, 34)$, $(33, 59)$
$(66, 118)$, $(71, 12$
$(132, 236)$, $(203,$
$(325, 581)$, $(528,$
$(731, 1307)$, $(125$
$(1787, 3195)$, $(25$
$(3249, 5809)$, $(50$
$(6823, 12199)$, $(1$
$(16895, 30207)$, $($

New observation:
Simple endgames work well
if $rm - qn = \Delta$
with, e.g., $\Delta = \pm 2^a 3^b$.
Often find very good chains.

Easy to find $(q, r)$
given $(m, n, \Delta)$:
standard ext-gcd computation.

What if $(m, n)$ not coprime?
Great! Exploit factor.

Try many good choices
for $(\Delta, q, r)$, keep best.

Example of new chain:
$(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, -1)$,
$(1, 1)$, $(1, 2)$, $(2, 3)$, $(3, 5)$,
$(4, 7)$, $(5, 9)$, $(9, 16)$, $(14, 25)$,
$(19, 34)$, $(33, 59)$, $(38, 68)$,
$(66, 118)$, $(71, 127)$, $(61, 109)$,
$(132, 236)$, $(203, 363)$, $(264, 472)$,
$(325, 581)$, $(528, 944)$,
$(731, 1307)$, $(1259, 2251)$,
$(1787, 3195)$, $(2518, 4502)$,
$(3249, 5809)$, $(5036, 9004)$,
$(6823, 12199)$, $(10072, 18008)$,
$(16895, 30207)$, $(26967, 48215)$.