Quantum algorithms for the subset-sum problem

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Joint work with:

Stacey Jeffery
University of Waterloo

Tanja Lange
Technische Universiteit Eindhoven

Alexander Meurer
Ruhr-Universität Bochum

Subset-sum example:
Is there a subsequence of
$(499, 852, 1927, 2535, 3596, 3608, 4688, 5989, 6385, 7353, 7650, 9413)$
having sum 36634?

Many variations: e.g.,
find such a subsequence
if one exists;
find such a subsequence
knowing that one exists;
allow range of sums;
coefficients outside $\{0, 1\}$; etc.

"Subset-sum problem";
"knapsack problem"; etc.

The lattice connection

Define $x_1 = 499, \ldots, x_{12} = 9413$.

Define $L \subseteq \mathbf{Z}^{12}$ as
$\{v : v_1 x_1 + \cdots + v_{12} x_{12} = 0\}$.

Define $u \in \mathbf{Z}^{12}$ as
$(70, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

If $J \subseteq \{1, 2, \ldots, 12\}$
and $\sum_{i \in J} x_i = 36634$ then
$v \in L$ where $v_i = u_i - [i \in J]$.

v is very close to u.
Reasonable to hope that
v is the closest vector in L to u.
Subset-sum algorithms $\approx$
codimension-1 CVP algorithms.

The coding connection

A weight-w subset-sum problem:
Is there a subsequence of
$(499, 852, 1927, 2535, 3596, 3608, 4688, 5989, 6385, 7353, 7650, 9413)$
having length w and sum 36634?

The coding connection

A weight-w subset-sum problem:
Is there a subsequence of
$(499, 852, 1927, 2535, 3596, 3608, 4688, 5989, 6385, 7353, 7650, 9413)$
having length w and sum 36634?

Replace $\mathbf{Z}$ with $(\mathbf{Z}/2)^m$:
Is there a subsequence of
$(499, 852, 1927, 2535, 3596, 3608, 4688, 5989, 6385, 7353, 7650, 9413)$
having length w and xor 1060?

This is the central algorithmic problem in coding theory.

Recent asymptotic news

Eurocrypt 2010
Howgrave-Graham–Joux:
subset-sum exponent ≈ 0.337.
(Incorrect claim: ≈ 0.311.)

Eurocrypt 2011
Becker–Coron–Joux:
subset-sum exponent ≈ 0.291.

Adaptations to decoding:
Asiacrypt 2011 May–Meurer–Thomae, Eurocrypt 2012 Becker–Joux–May–Meurer.

Post-quantum subset sum

Claimed in TCC 2010
Lyubashevsky–Palacio–Segev
"Public-key cryptographic
primitives provably
as secure as subset sum":

There are "currently no known
quantum algorithms that perform
better than classical ones
on the subset sum problem".

Hmmm. What's the best
quantum subset-sum exponent?

Quantum search (0.5)

Assume that function f
has n-bit input, unique root.

Generic brute-force search
finds this root using
$\approx 2^n$ evaluations of f.

1996 Grover method
finds this root using
$\approx 2^{0.5n}$ quantum evaluations of f
on superpositions of inputs.

Cost of quantum evaluation of f
$\approx$ cost of evaluation of f
if cost counts qubit "operations".

Easily adapt to handle
different # of roots,
and # not known in advance.
Faster if # is large,
but typically # is not very large.
Most interesting: $\# \in \{0, 1\}$.

Easily adapt to handle
different # of roots,
and # not known in advance.
Faster if # is large,
but typically # is not very large.
Most interesting: $\# \in \{0, 1\}$.

Apply to the function
$J \mapsto \Sigma(J) - t$ where
$\Sigma(J) = \sum_{i \in J} x_i$.

Cost $2^{0.5n}$ to find root (i.e.,
to find indices of subsequence
of $x_1, \ldots, x_n$ with sum t)
or to decide that no root exists.
We suppress poly factors in cost.

Algorithm details for unique root:

Represent $J \subseteq \{1, \ldots, n\}$ as an integer between 0 and $2^n - 1$.

n bits are enough space to store one such integer.

n qubits store much more, a superposition over sets J: 2^n complex amplitudes $a_0, \ldots, a_{2^n-1}$ with $|a_0|^2 + \cdots + |a_{2^n-1}|^2 = 1$. Measuring these n qubits has chance $|a_J|^2$ to produce J.

Start from uniform superposition, i.e., $a_J = 1/2^{n/2}$ for all J.

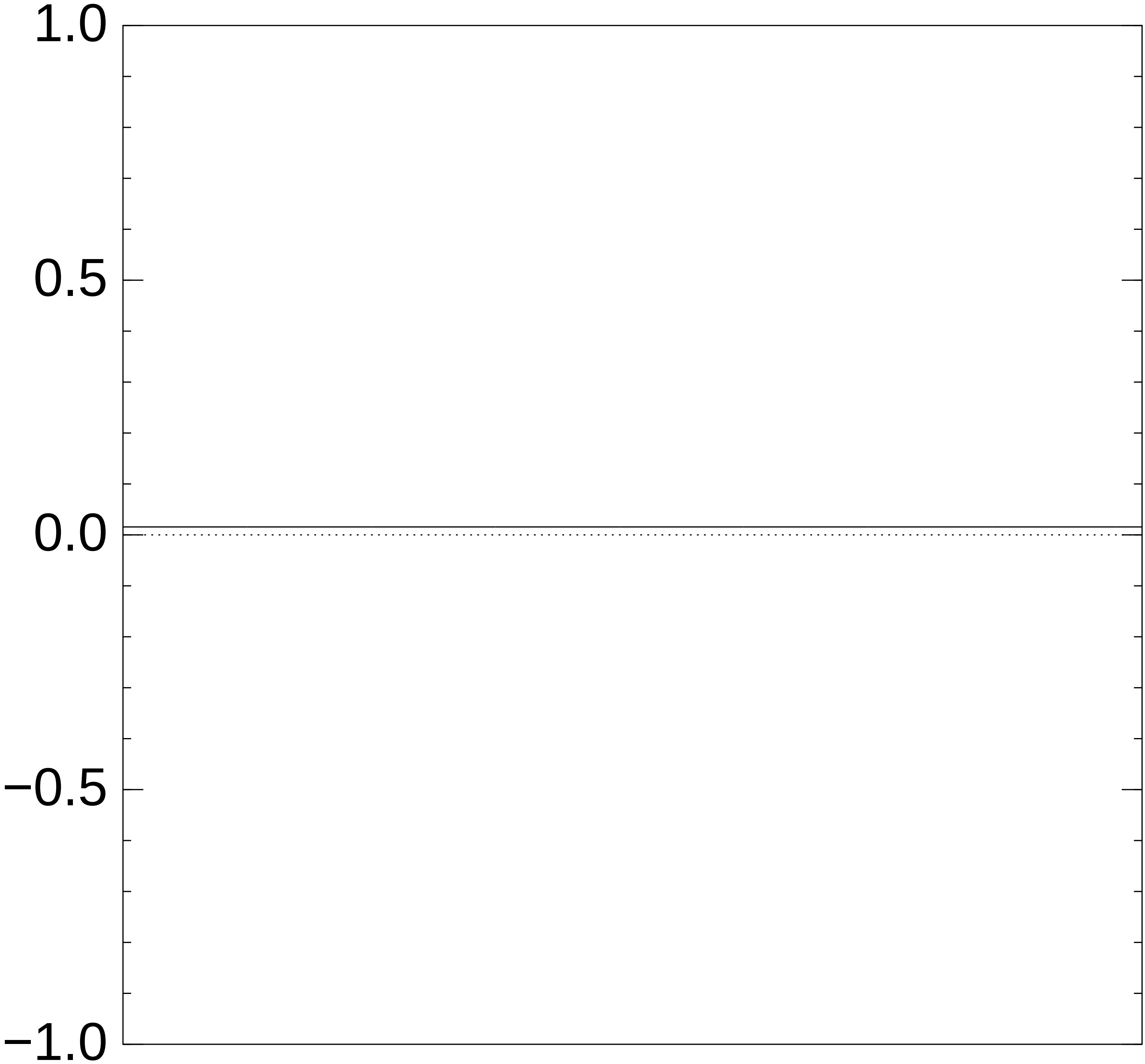
Step 1: Set $a \leftarrow b$ where
$b_J = -a_J$ if $\Sigma(J) = t$,
$b_J = a_J$ otherwise.
This is about as easy
as computing Σ.

Step 2: "Grover diffusion".
Set $a \leftarrow b$ where
$b_J = -a_J + (2/2^n) \sum_I a_I$.
This is also easy.

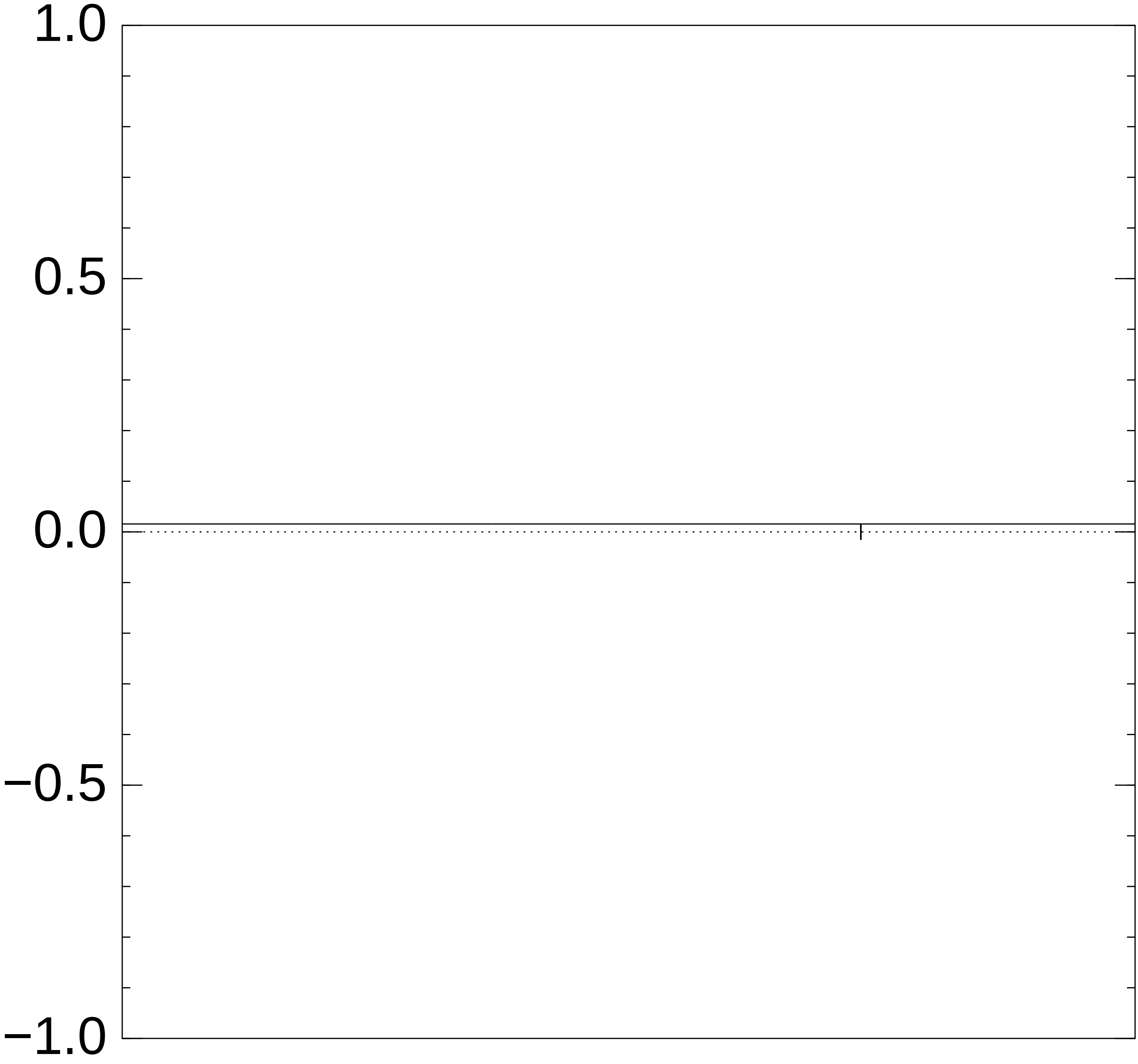
Repeat steps 1 and 2
about $0.58 \cdot 2^{0.5n}$ times.

Measure the n qubits.
With high probability this finds
the unique J such that $\Sigma(J) = t$.

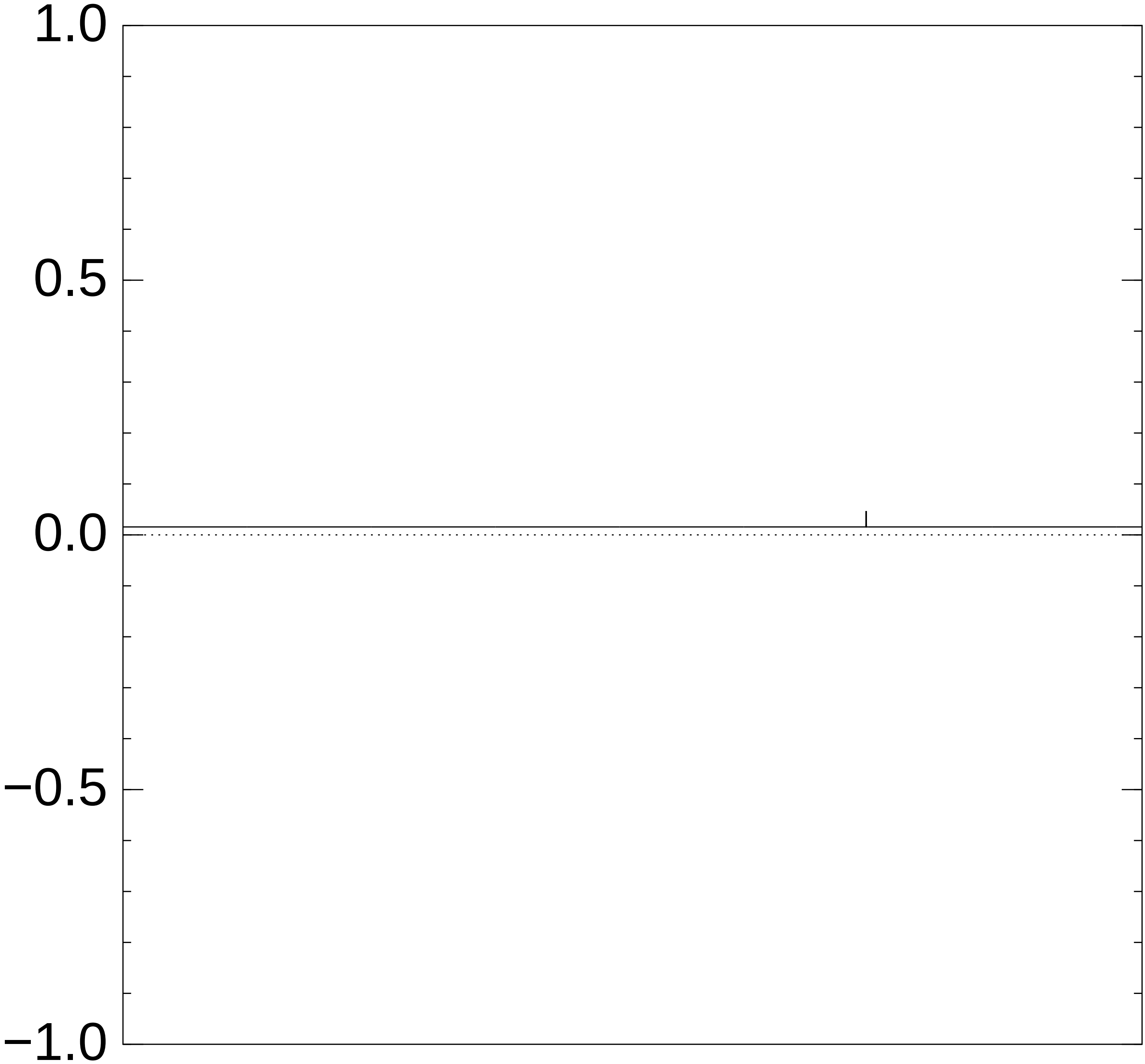
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after 0 steps:



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after Step 1:



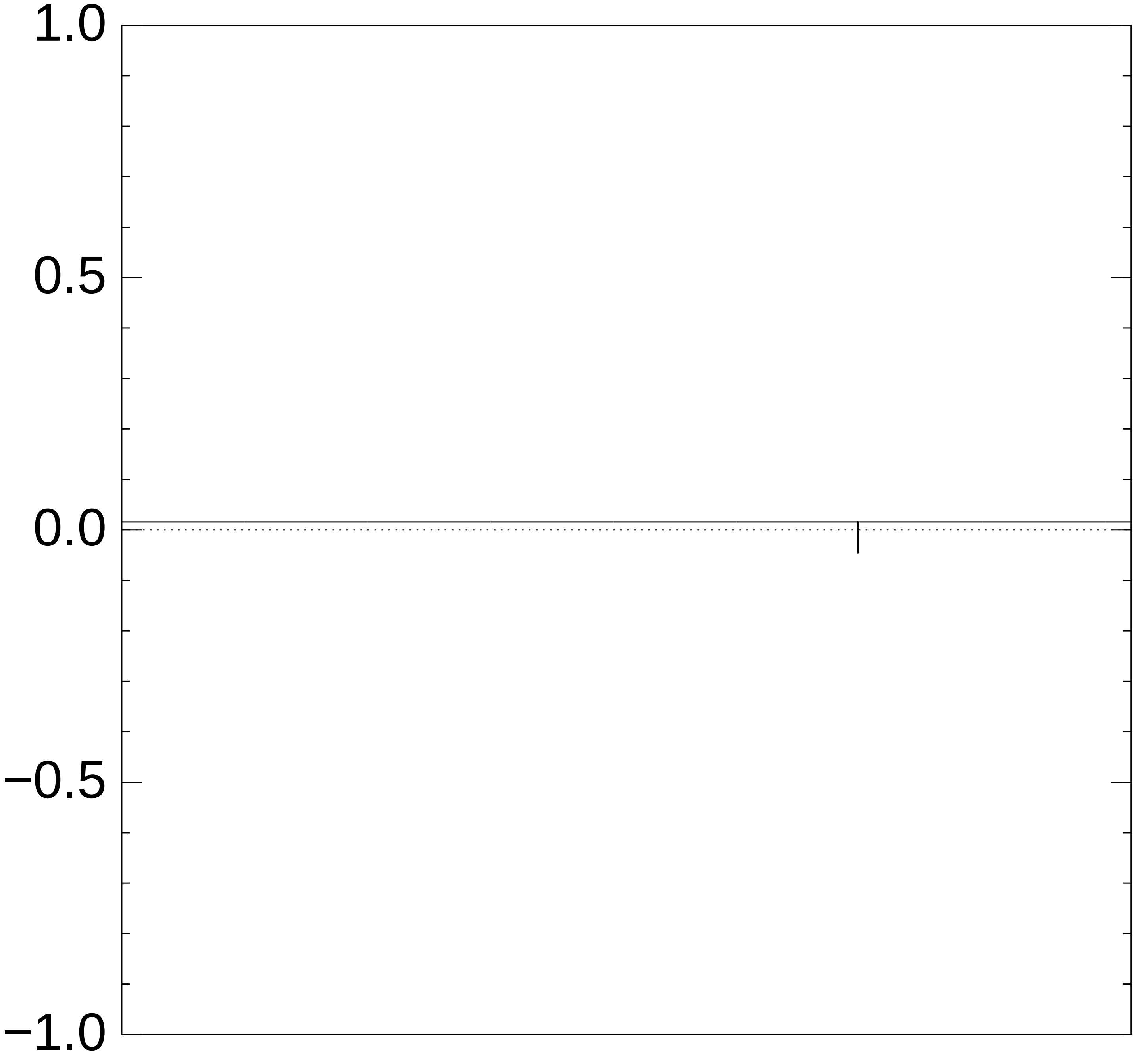
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after Step 1 + Step 2:



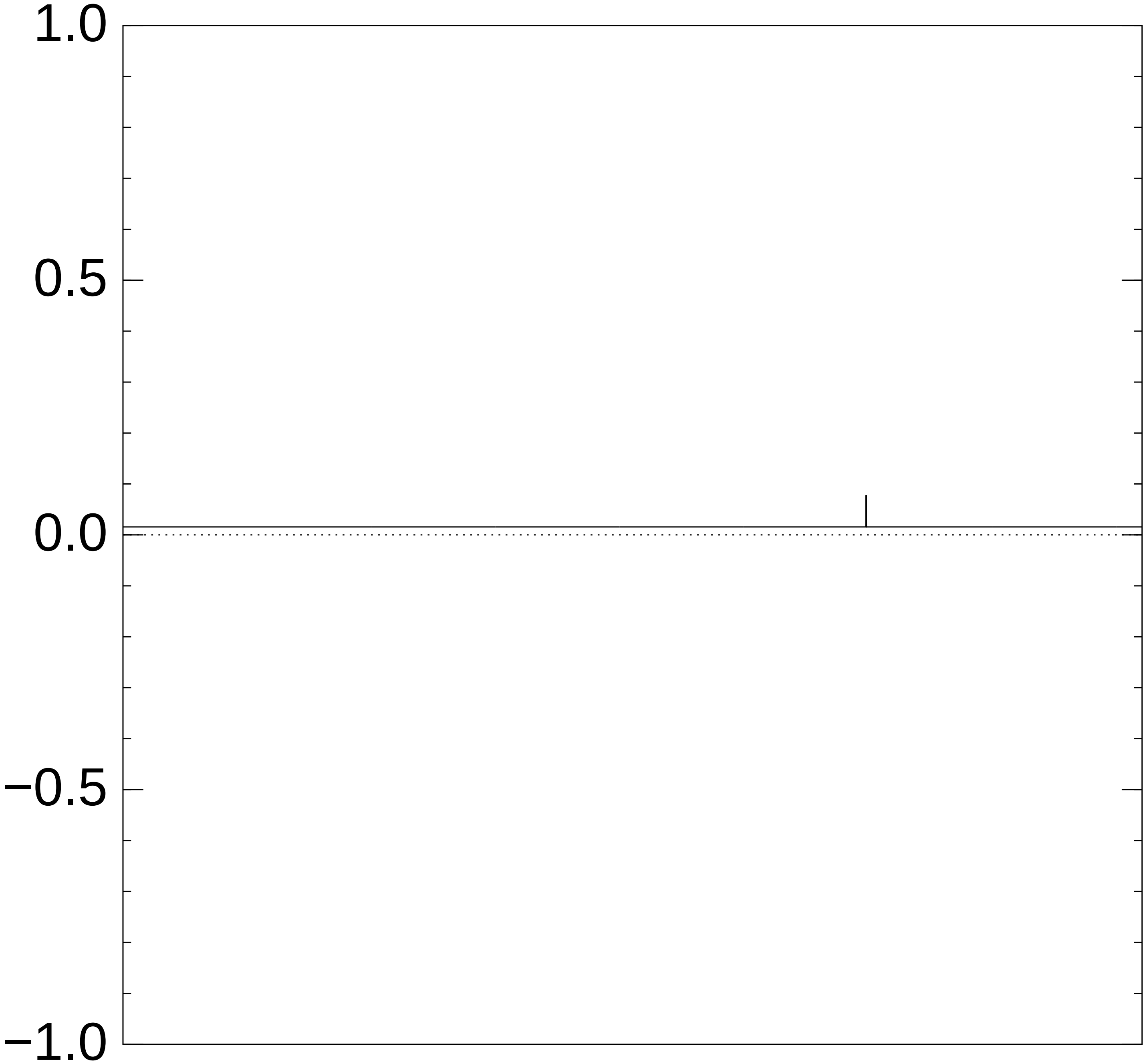
Graph of $J \mapsto a_J$

for 36634 example with $n = 12$

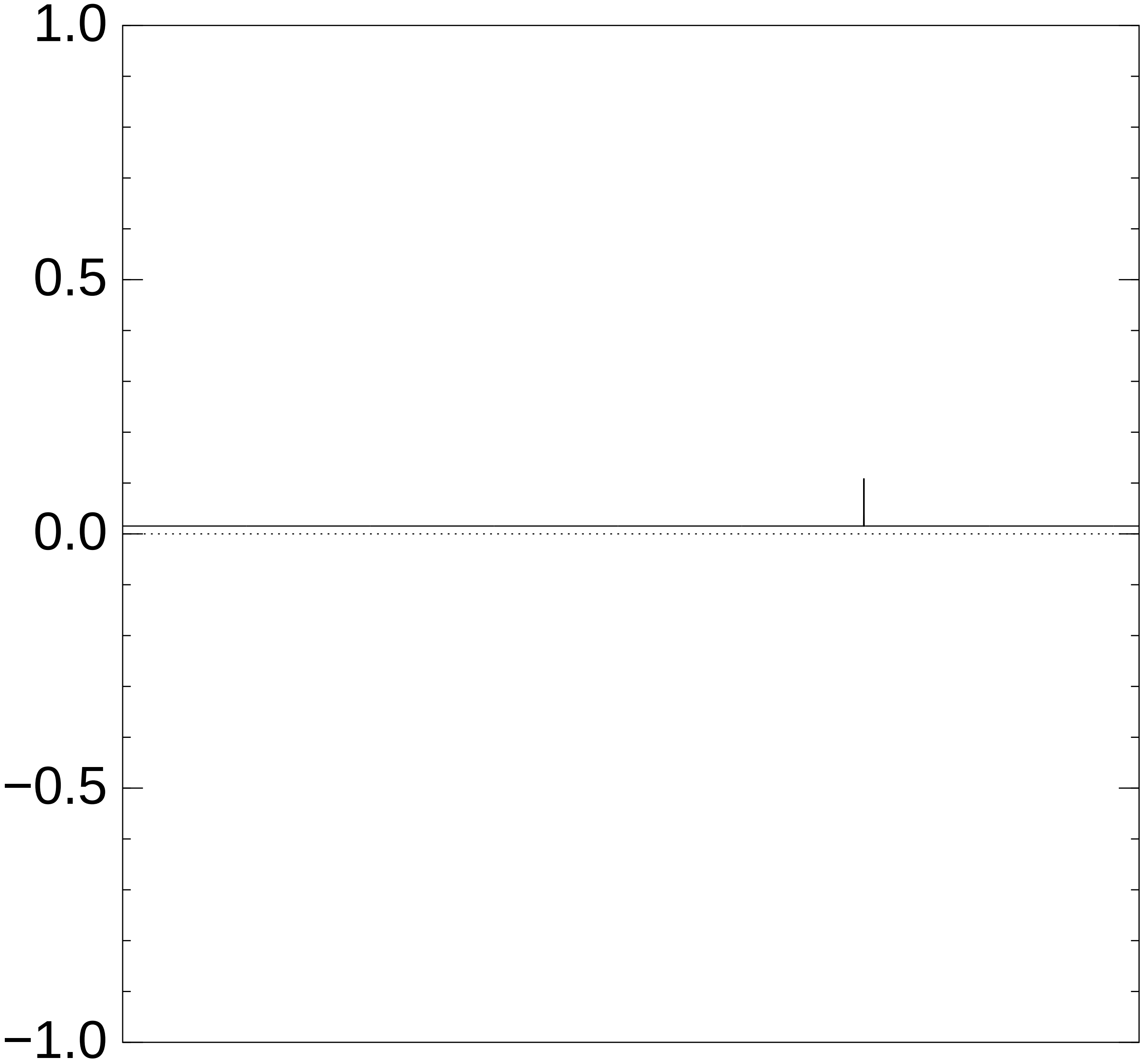
after Step $1 +$ Step $2 +$ Step 1:



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $2 \times (\text{Step } 1 + \text{Step } 2)$:



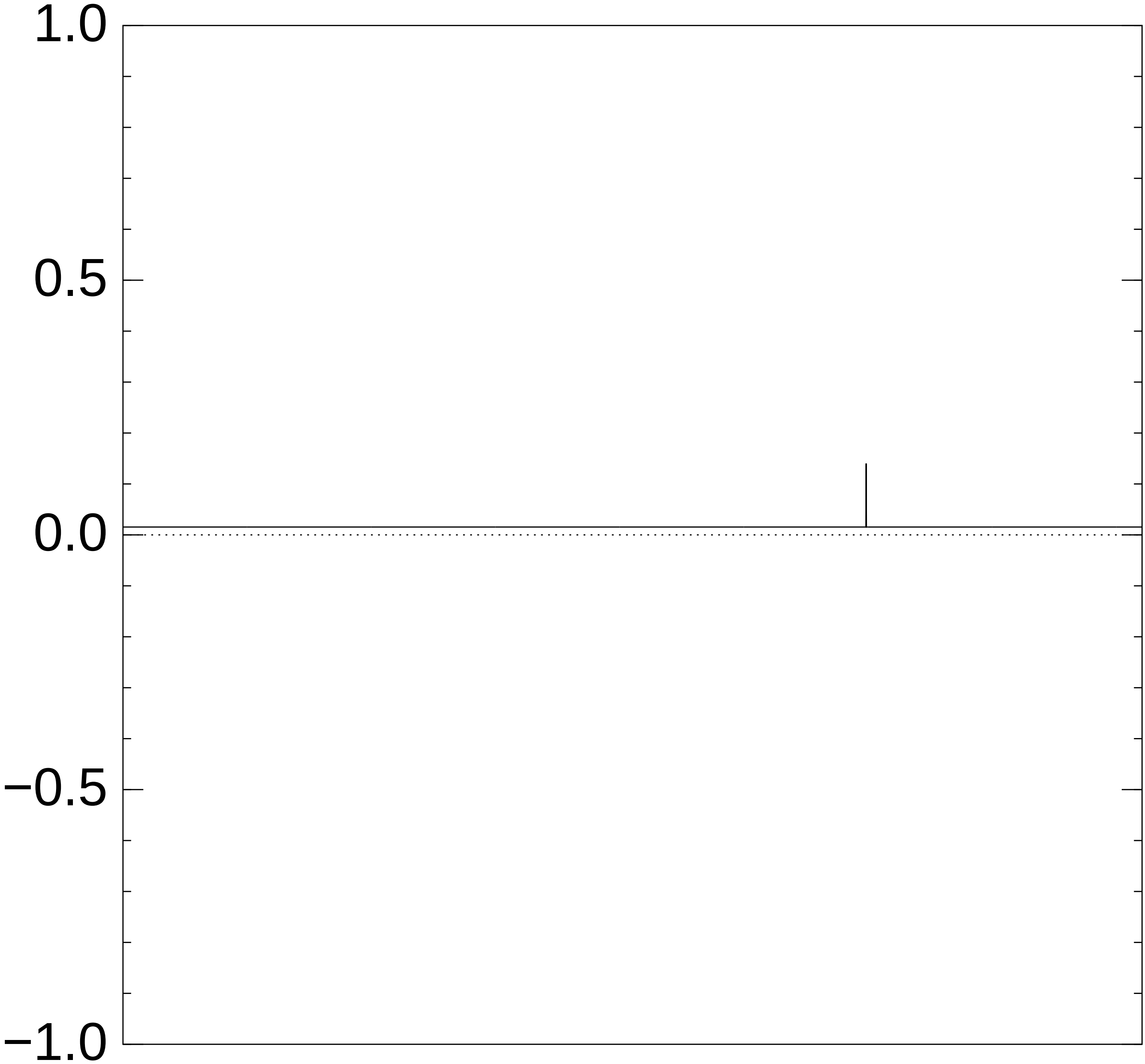
Graph of $J \mapsto a_J$ for 36634 example with $n = 12$ after $3 \times (\text{Step } 1 + \text{Step } 2)$:



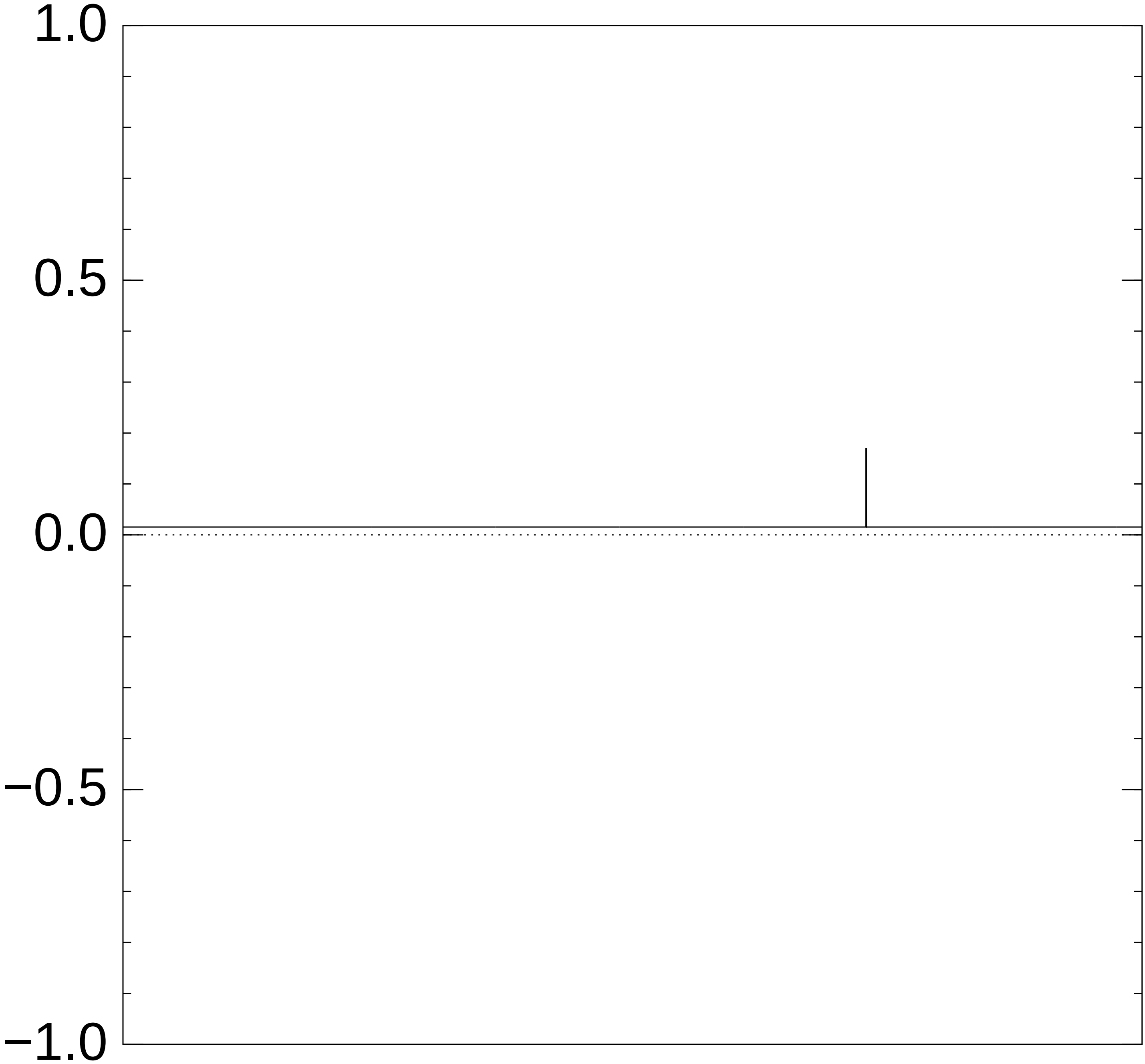
Graph of $J \mapsto a_J$

for 36634 example with $n = 12$

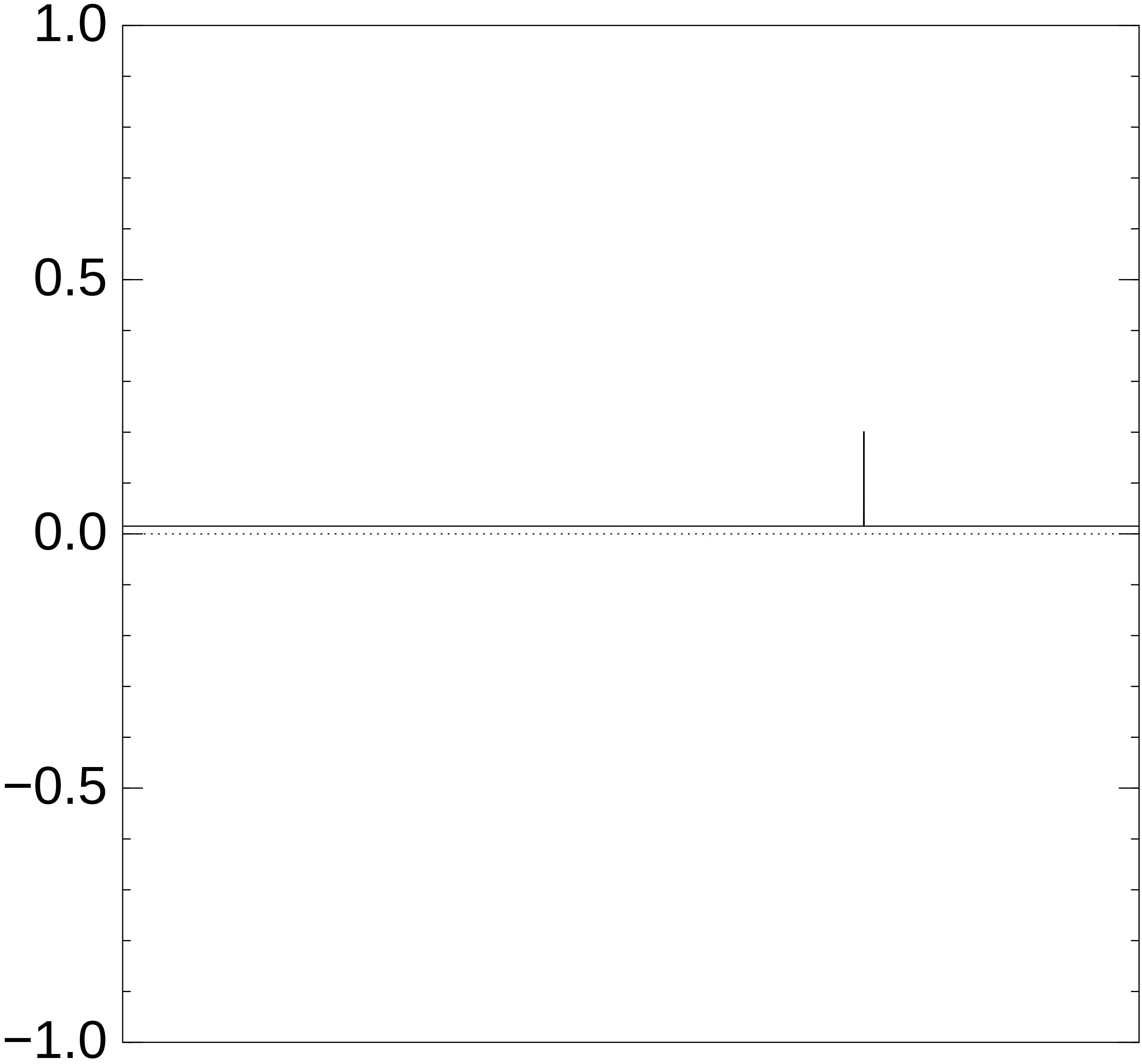
after $4 \times (\text{Step } 1 + \text{Step } 2)$:



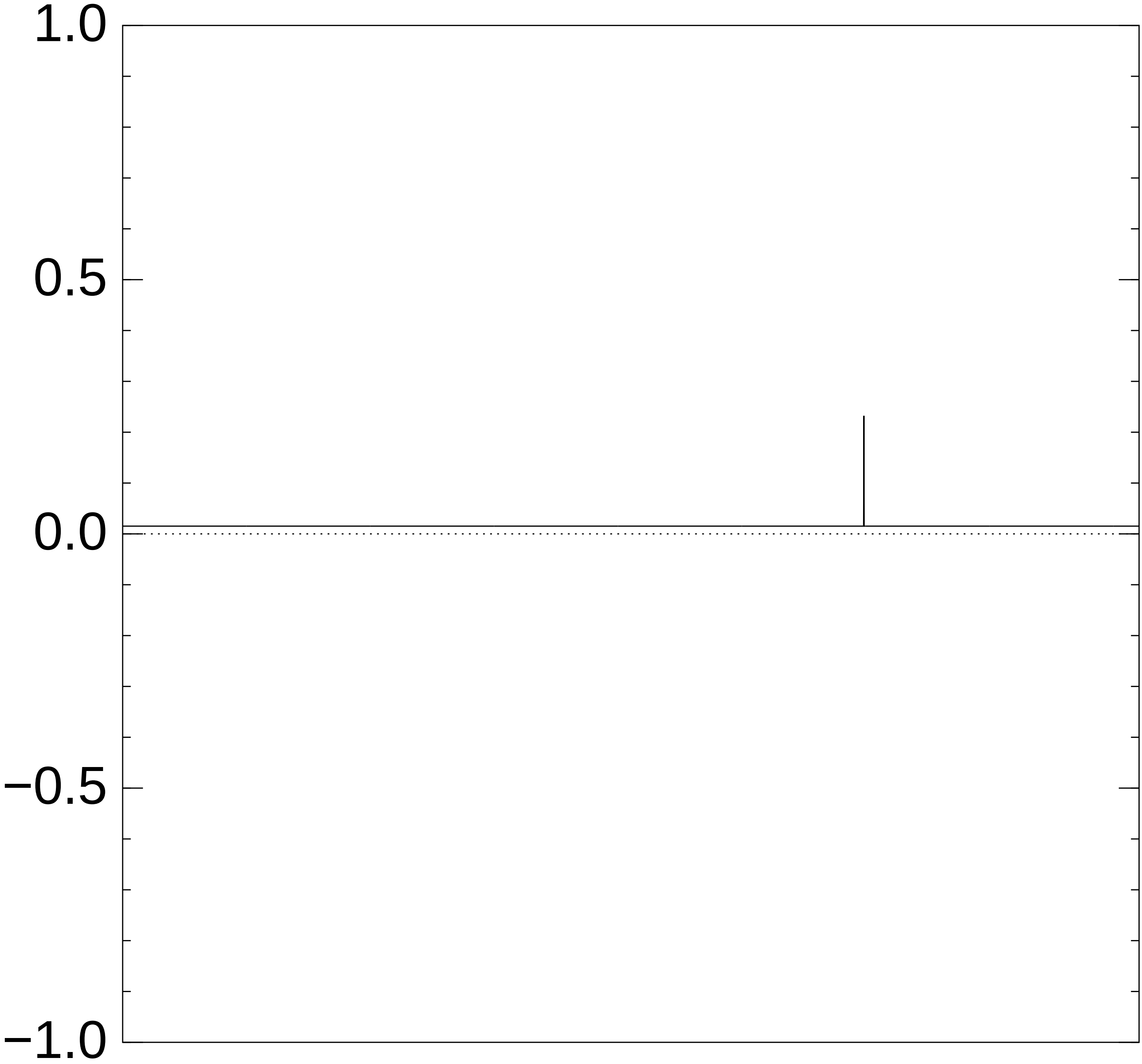
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $5 \times$ (Step $1 +$ Step 2):



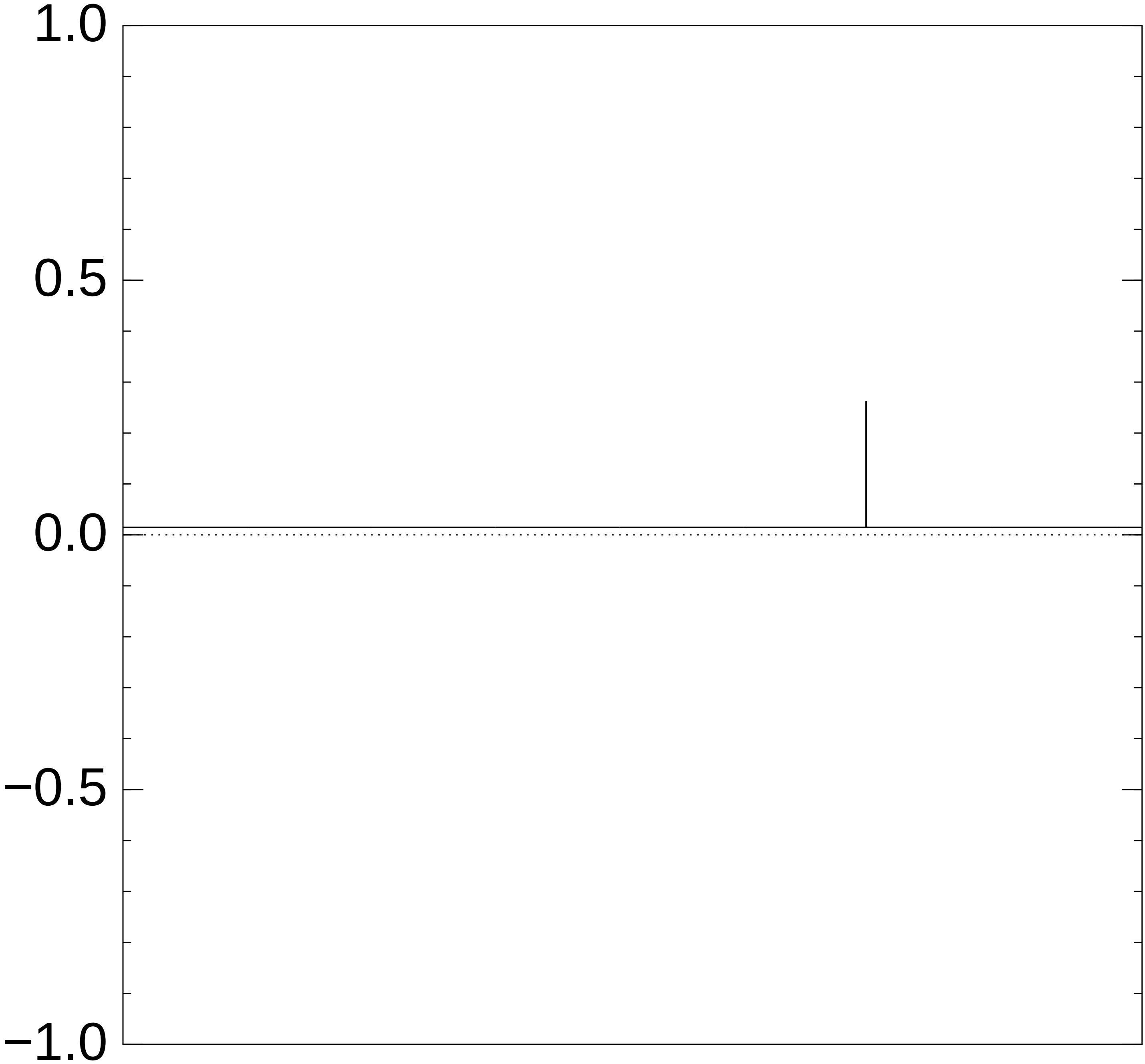
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $6 \times (\text{Step } 1 + \text{Step } 2)$:



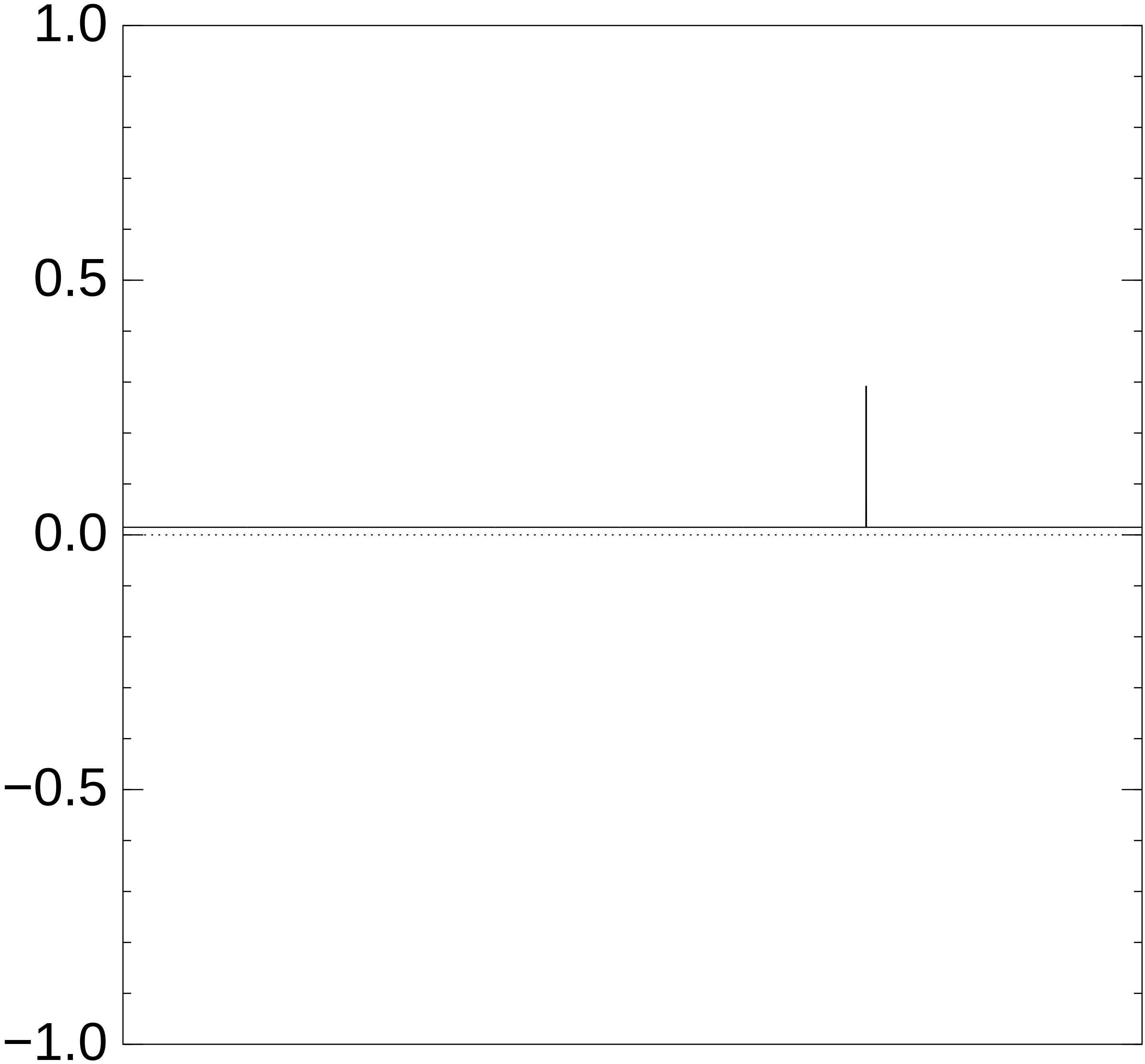
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $7 \times$ (Step $1 +$ Step 2):



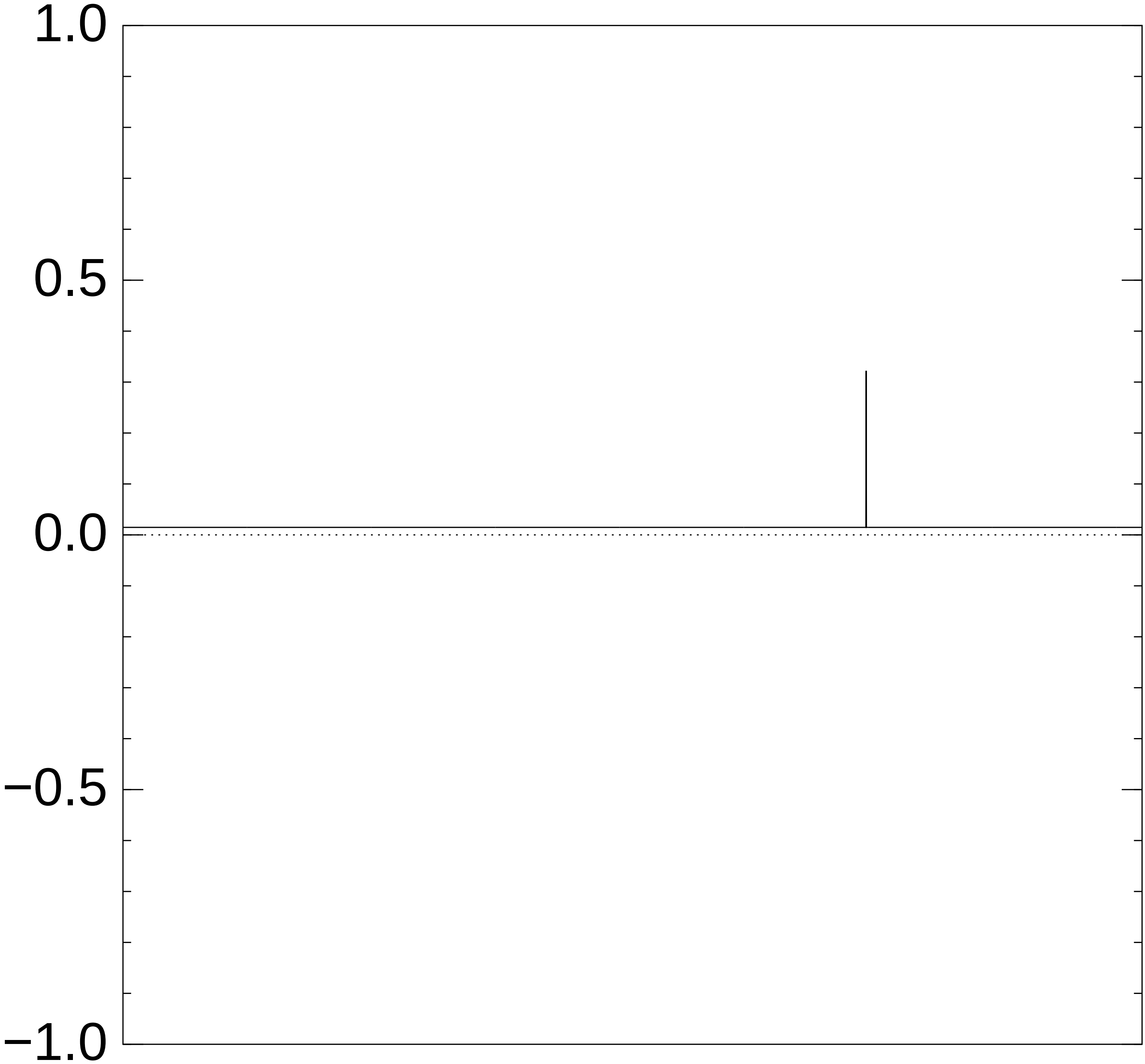
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $8 \times (\text{Step } 1 + \text{Step } 2)$:



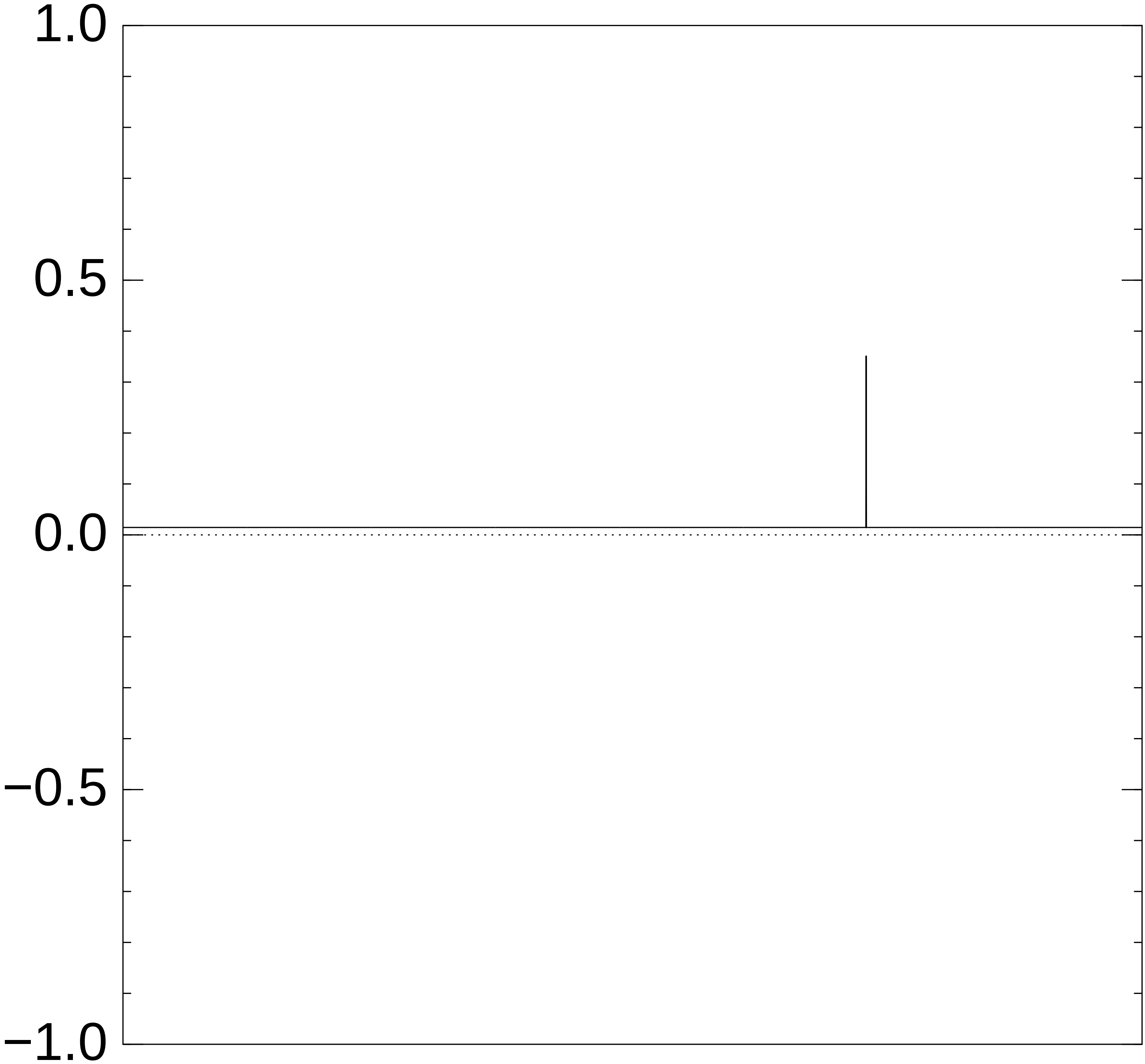
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $9 \times (\text{Step } 1 + \text{Step } 2)$:



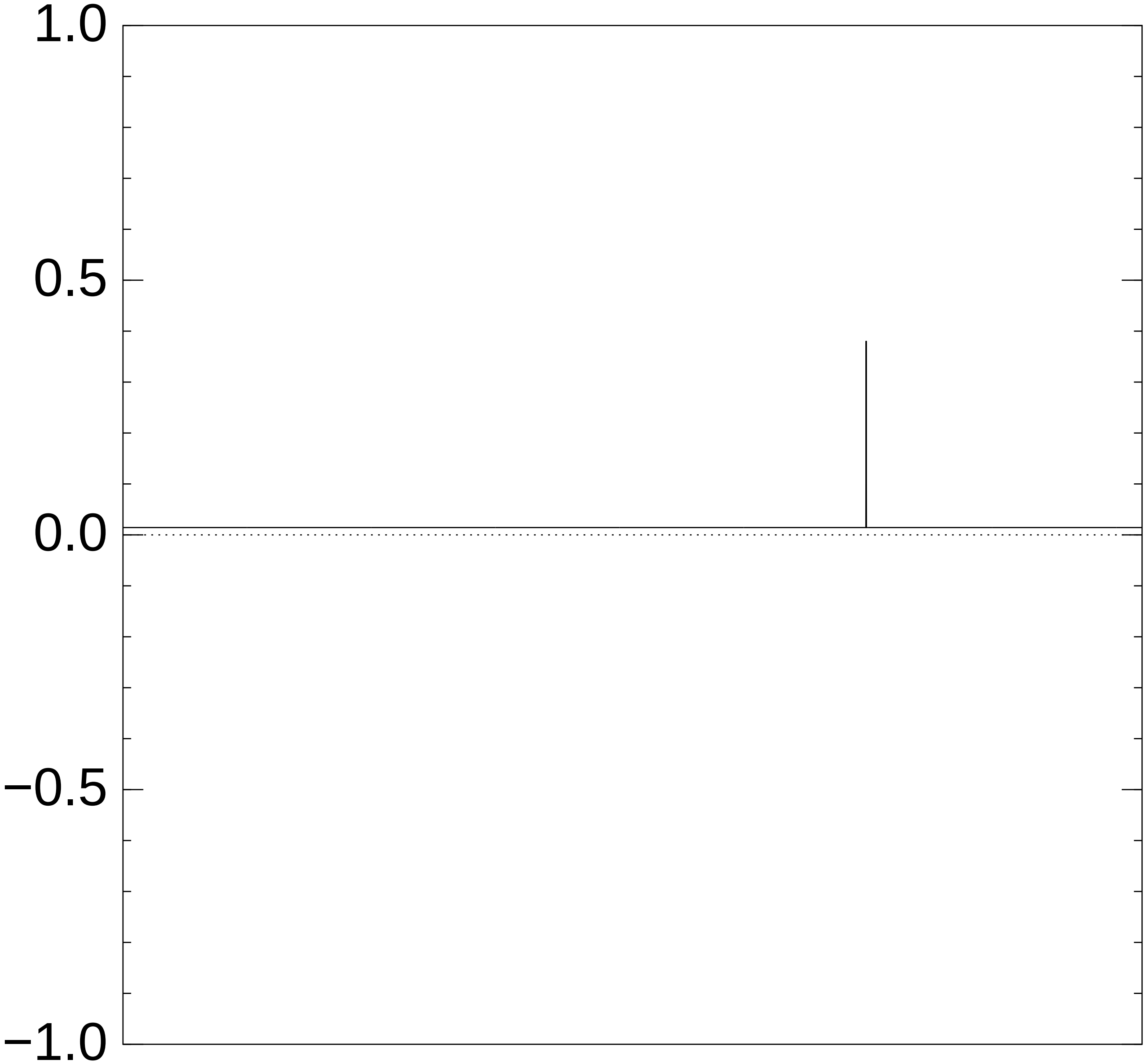
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $10 \times$ (Step $1 +$ Step 2):



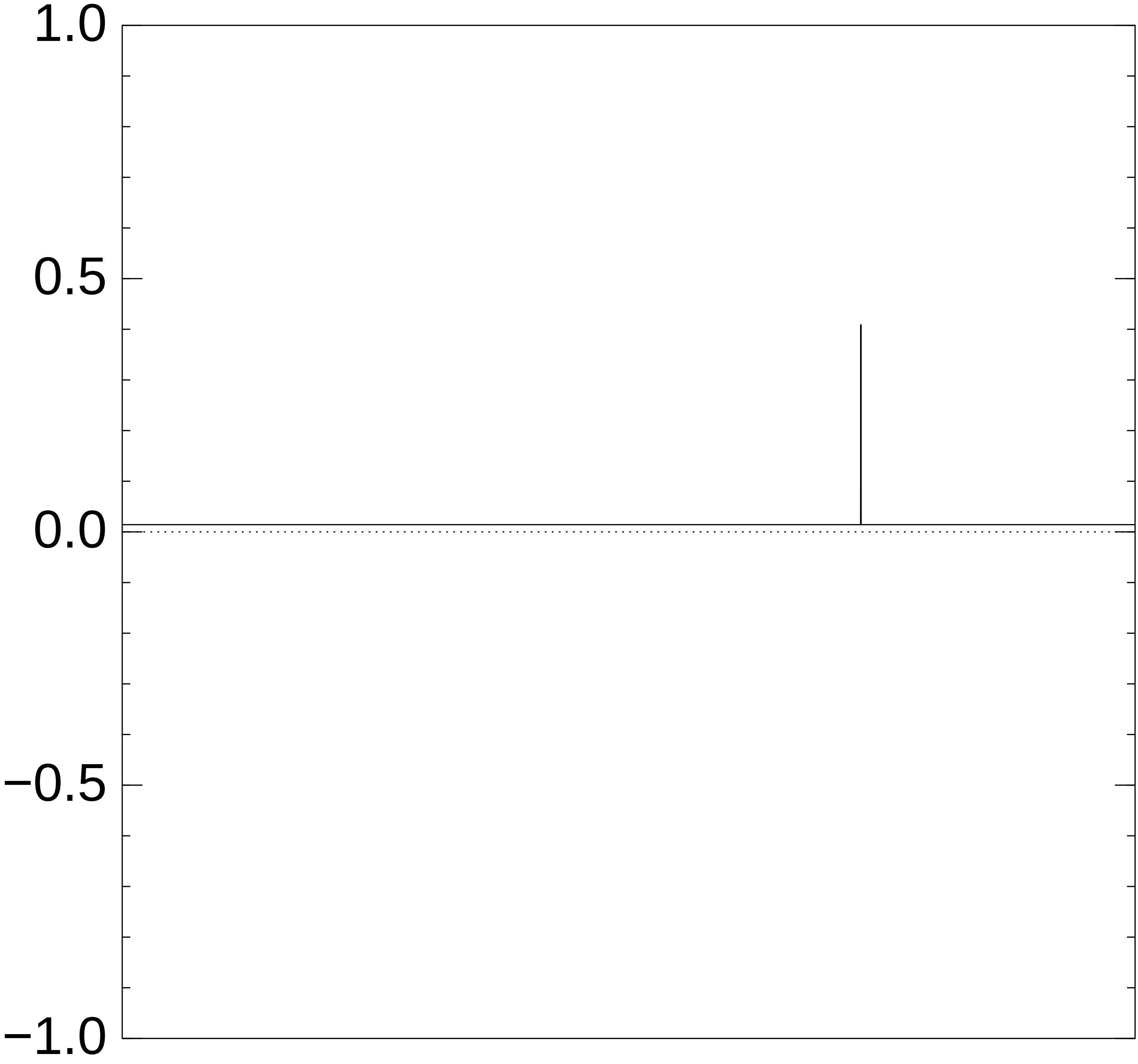
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $11 \times$ (Step $1 +$ Step 2):



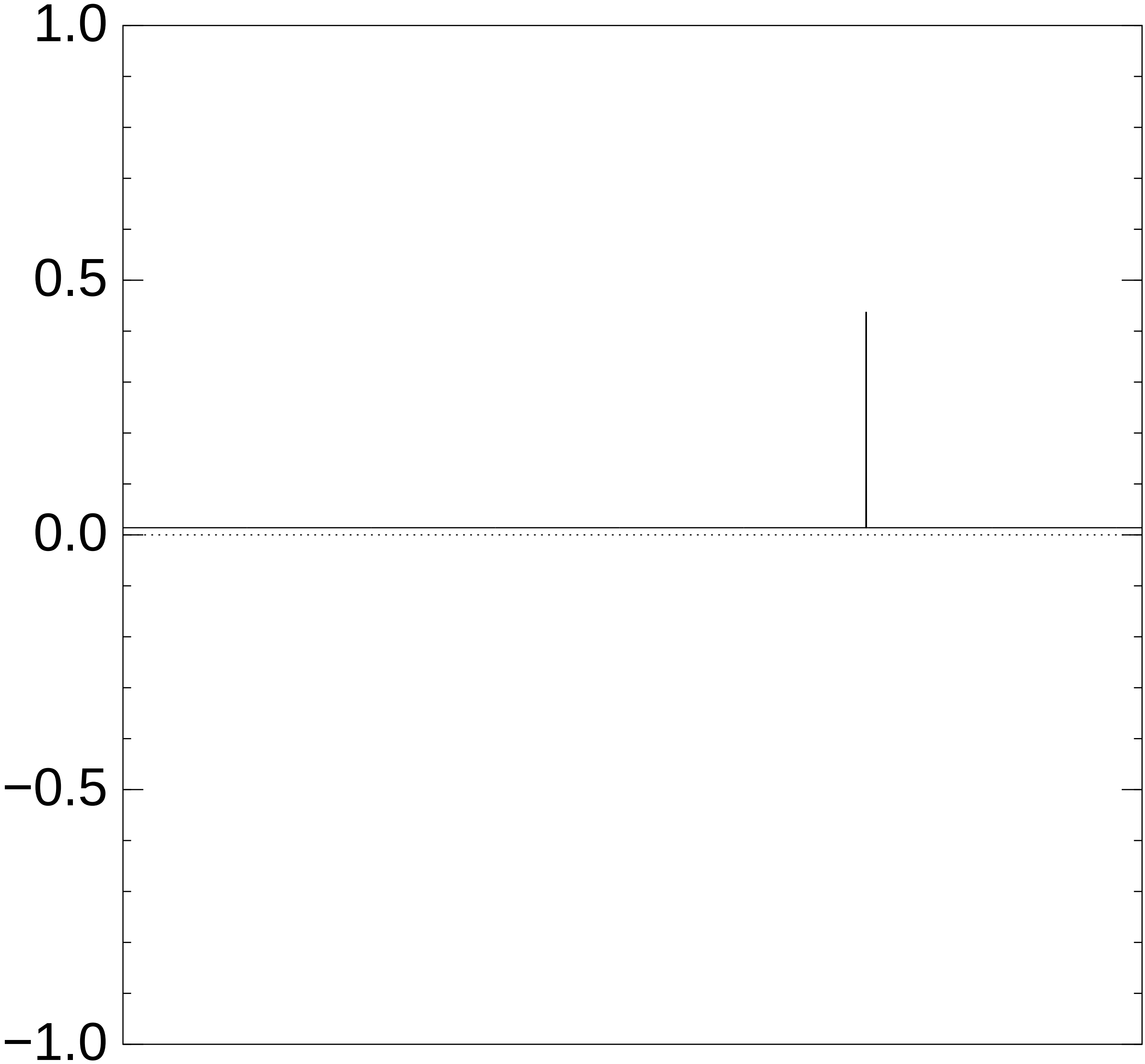
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $12 \times (\text{Step } 1 + \text{Step } 2)$:



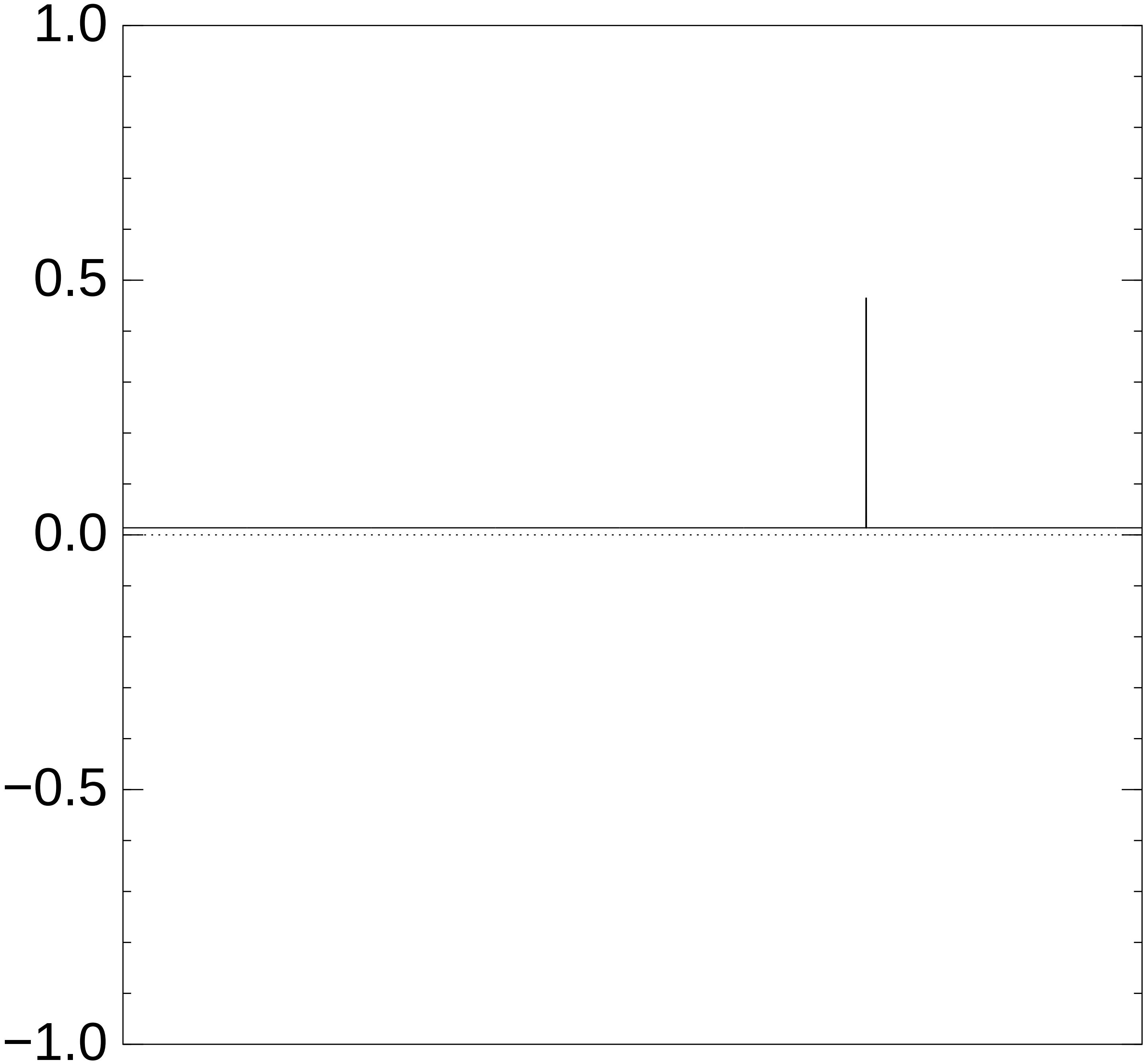
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $13 \times$ (Step $1 +$ Step 2):



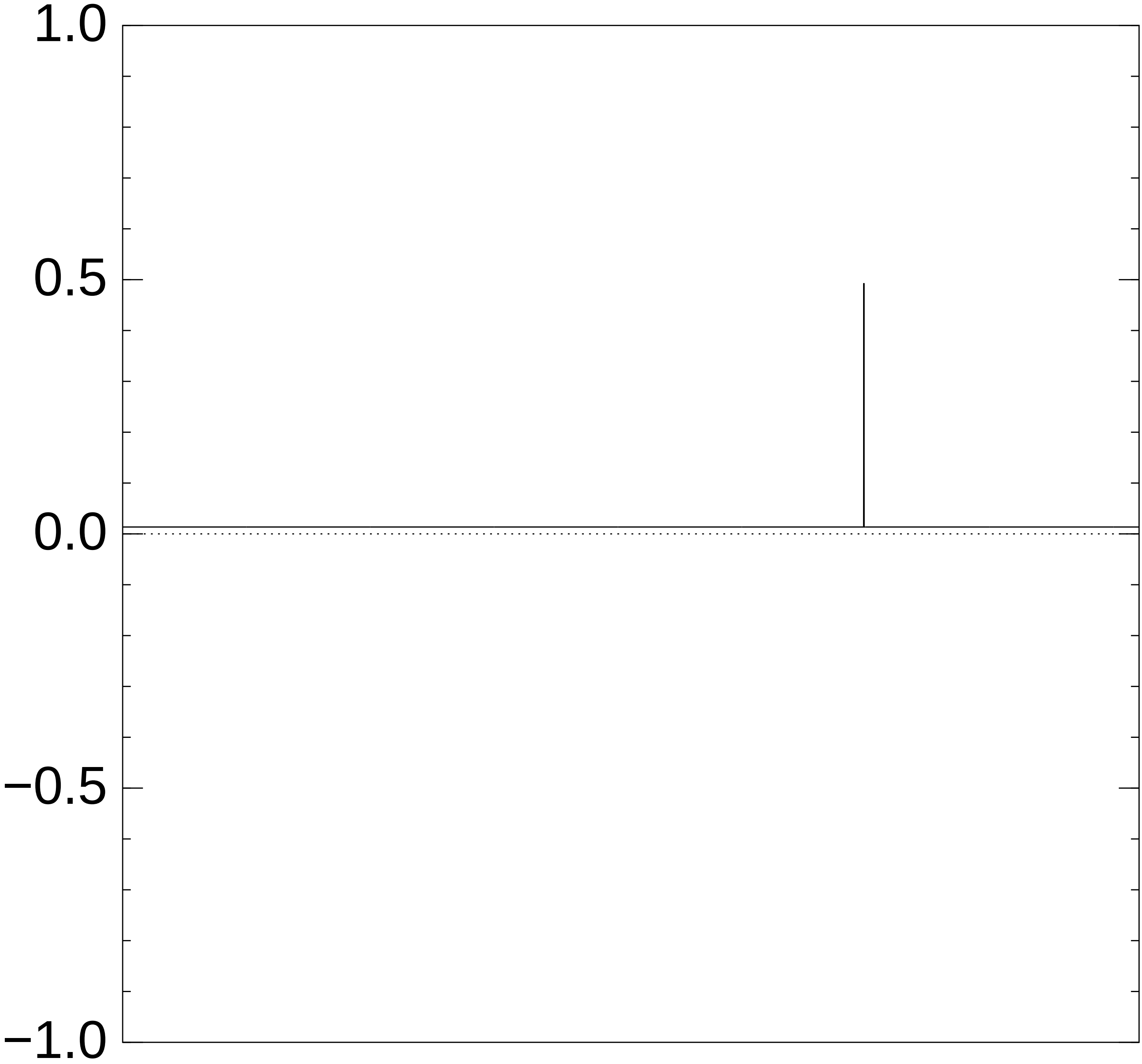
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $14 \times$ (Step $1 +$ Step 2):



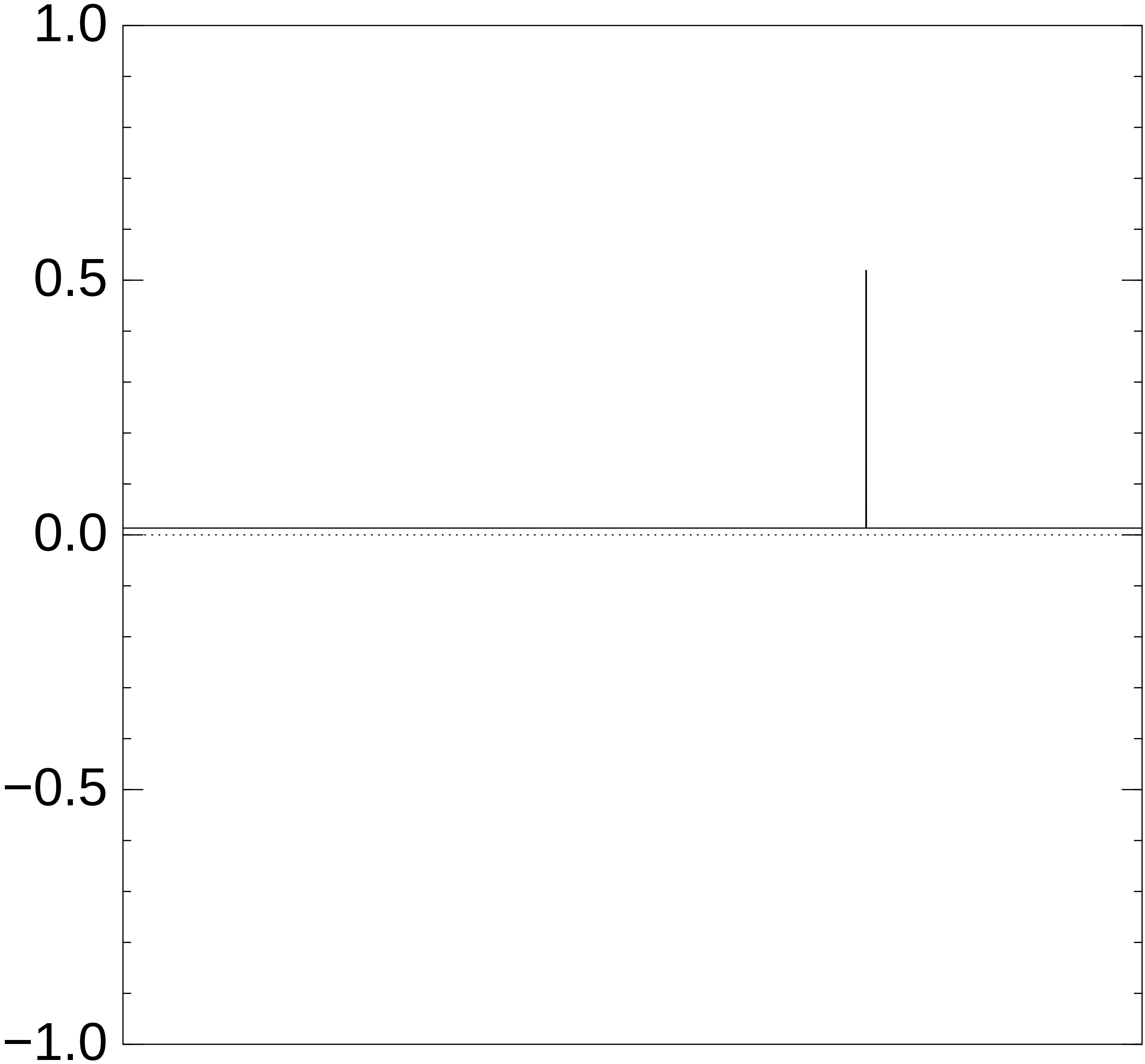
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $15 \times$ (Step $1 +$ Step 2):



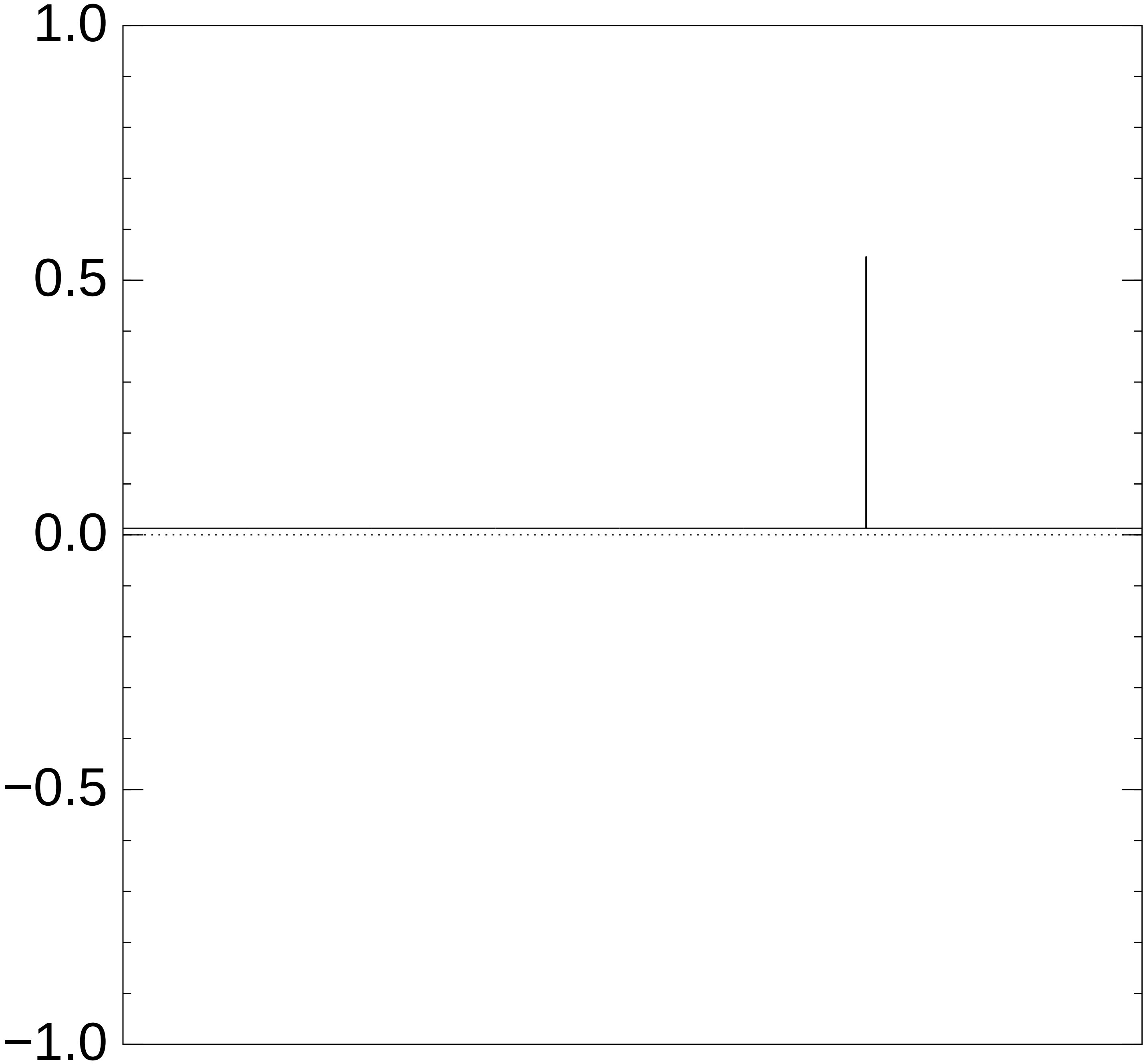
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $16 \times (\text{Step } 1 + \text{Step } 2)$:



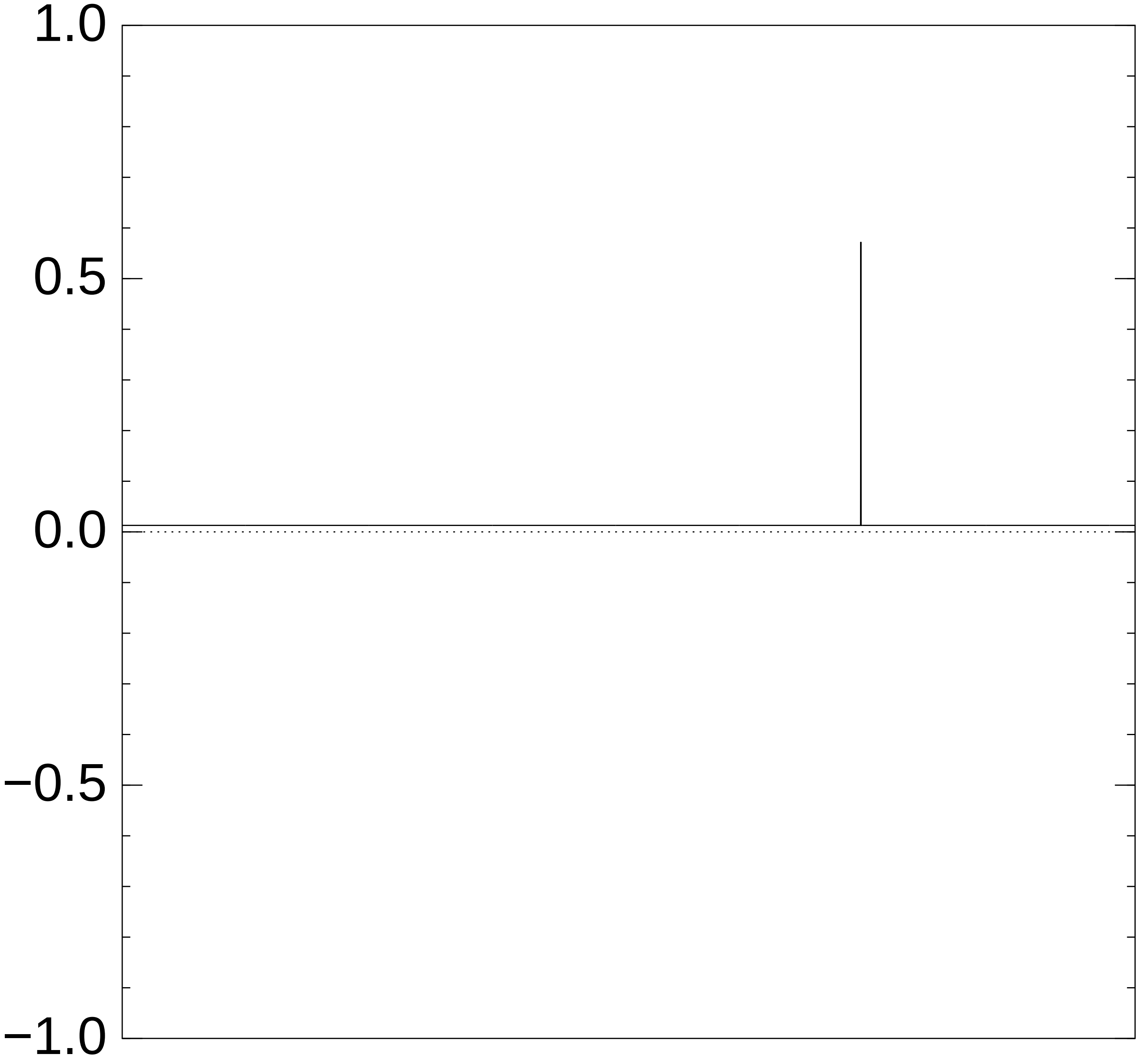
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $17 \times$ (Step $1 +$ Step 2):



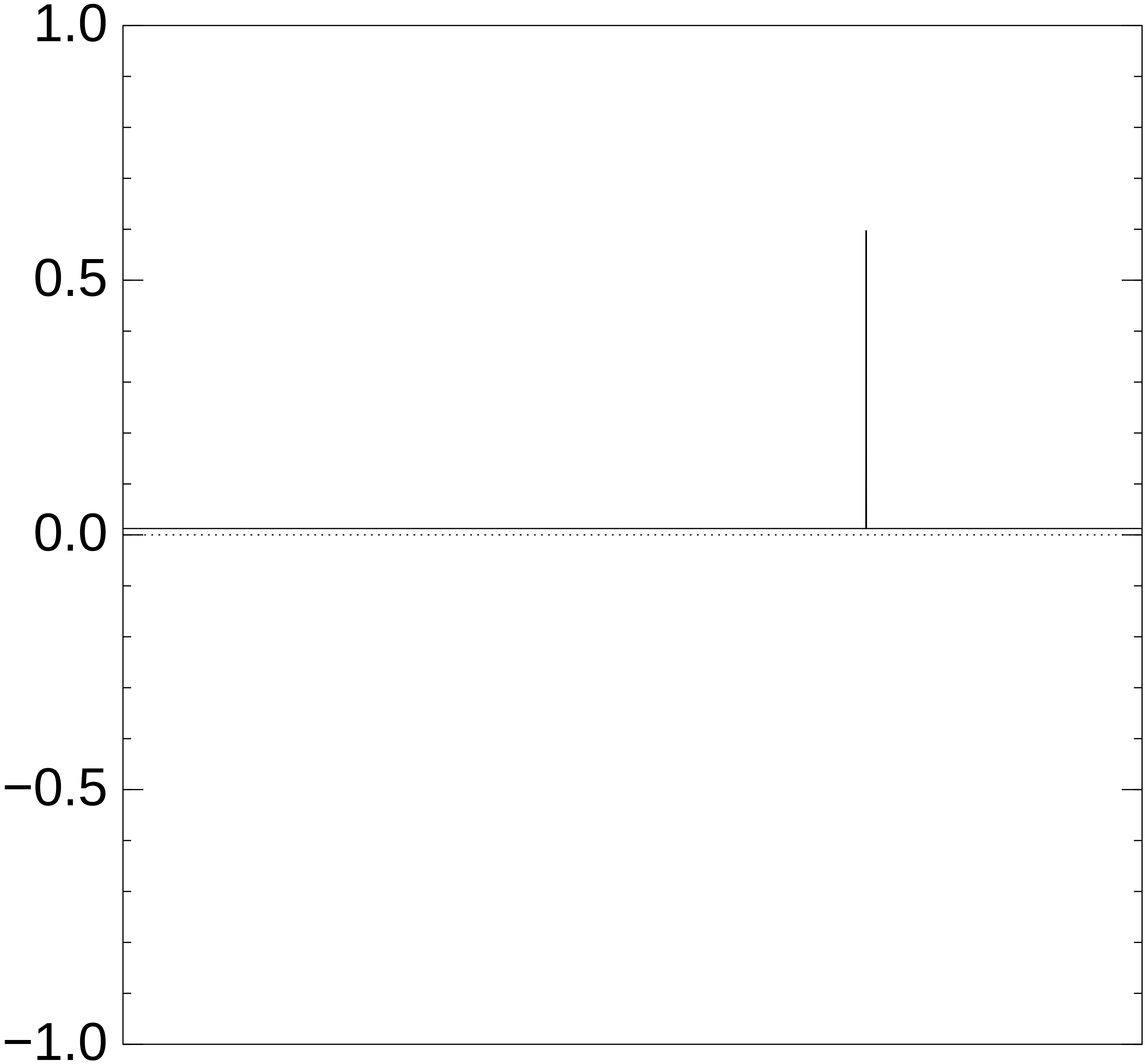
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $18 \times$ (Step $1 +$ Step 2):



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $19 \times (\text{Step } 1 + \text{Step } 2)$:



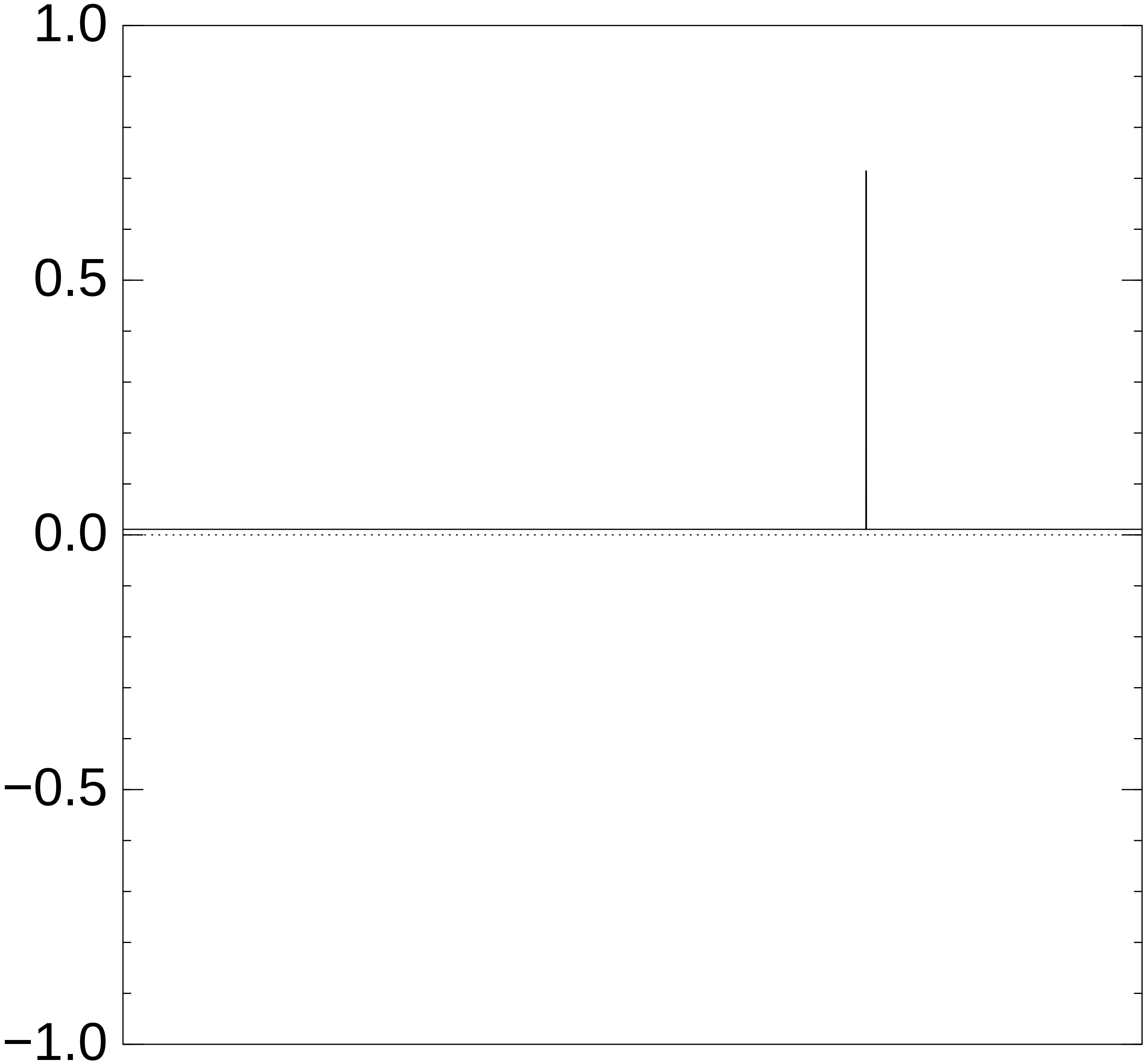
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $20 \times (\text{Step } 1 + \text{Step } 2)$:



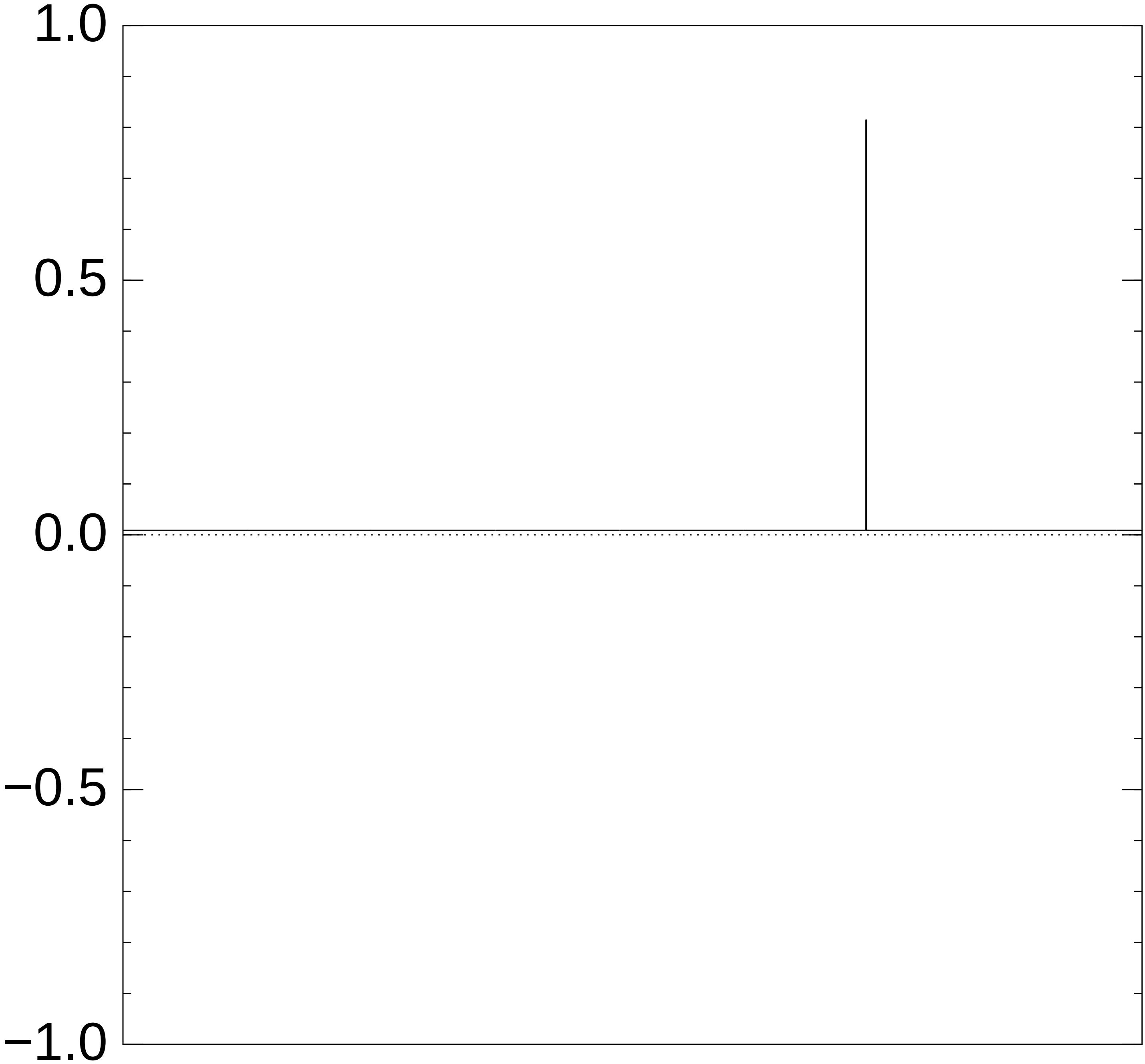
Graph of $J \mapsto a_J$

for 36634 example with $n = 12$

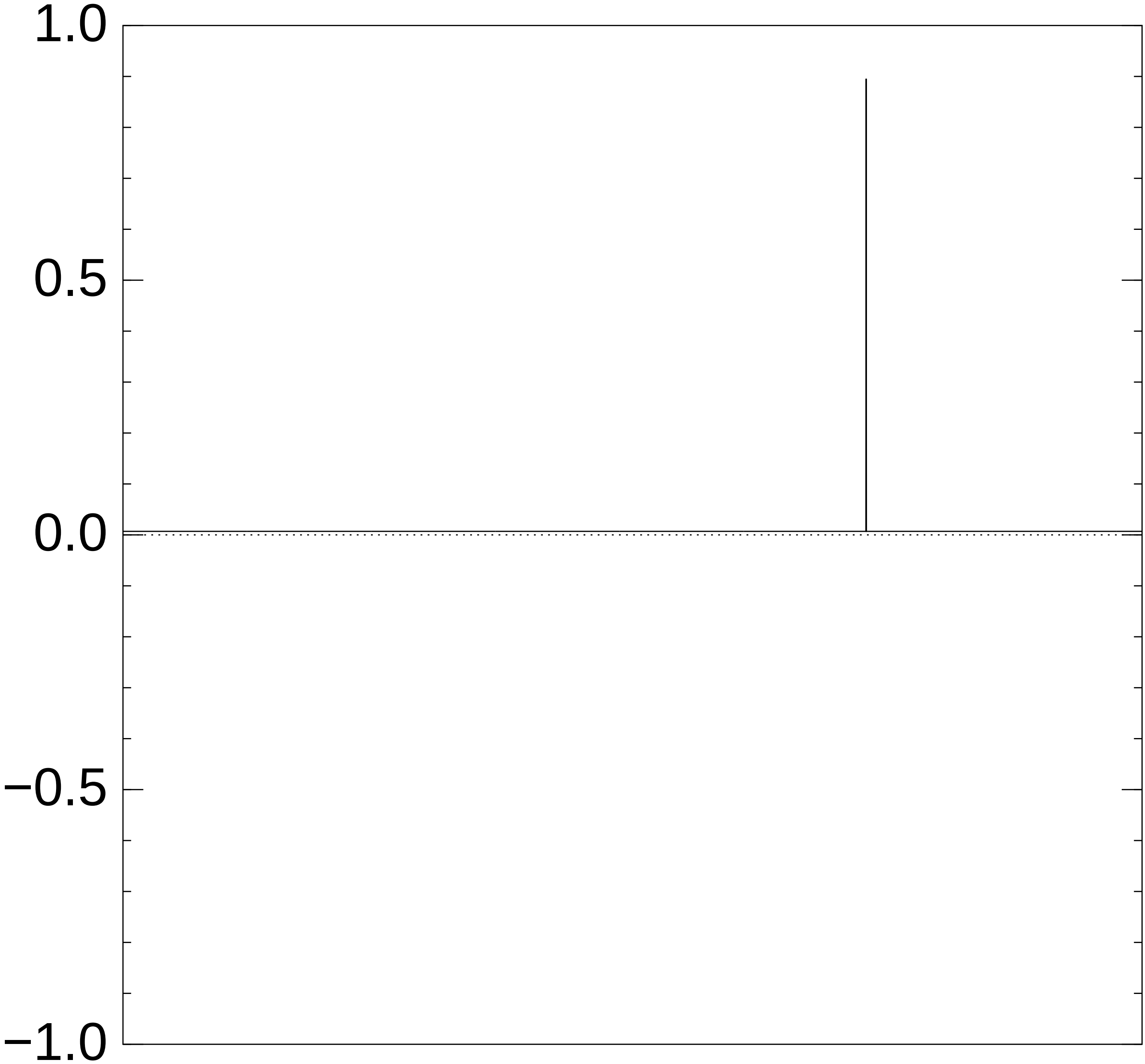
after $25 \times (\text{Step } 1 + \text{Step } 2)$:



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $30 \times$ (Step $1 +$ Step 2):

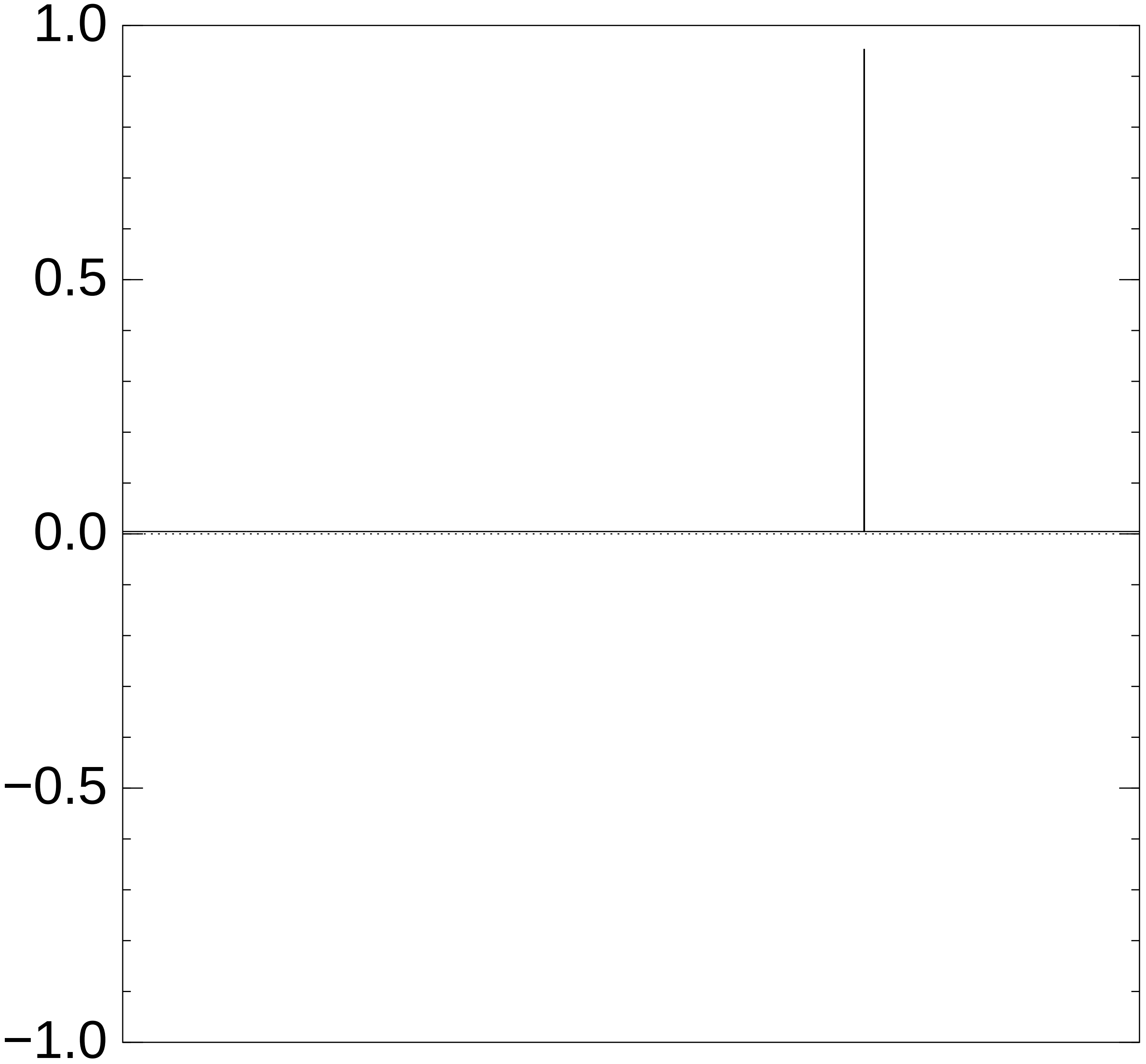


Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $35 \times (\text{Step } 1 + \text{Step } 2)$:



Good moment to stop, measure.

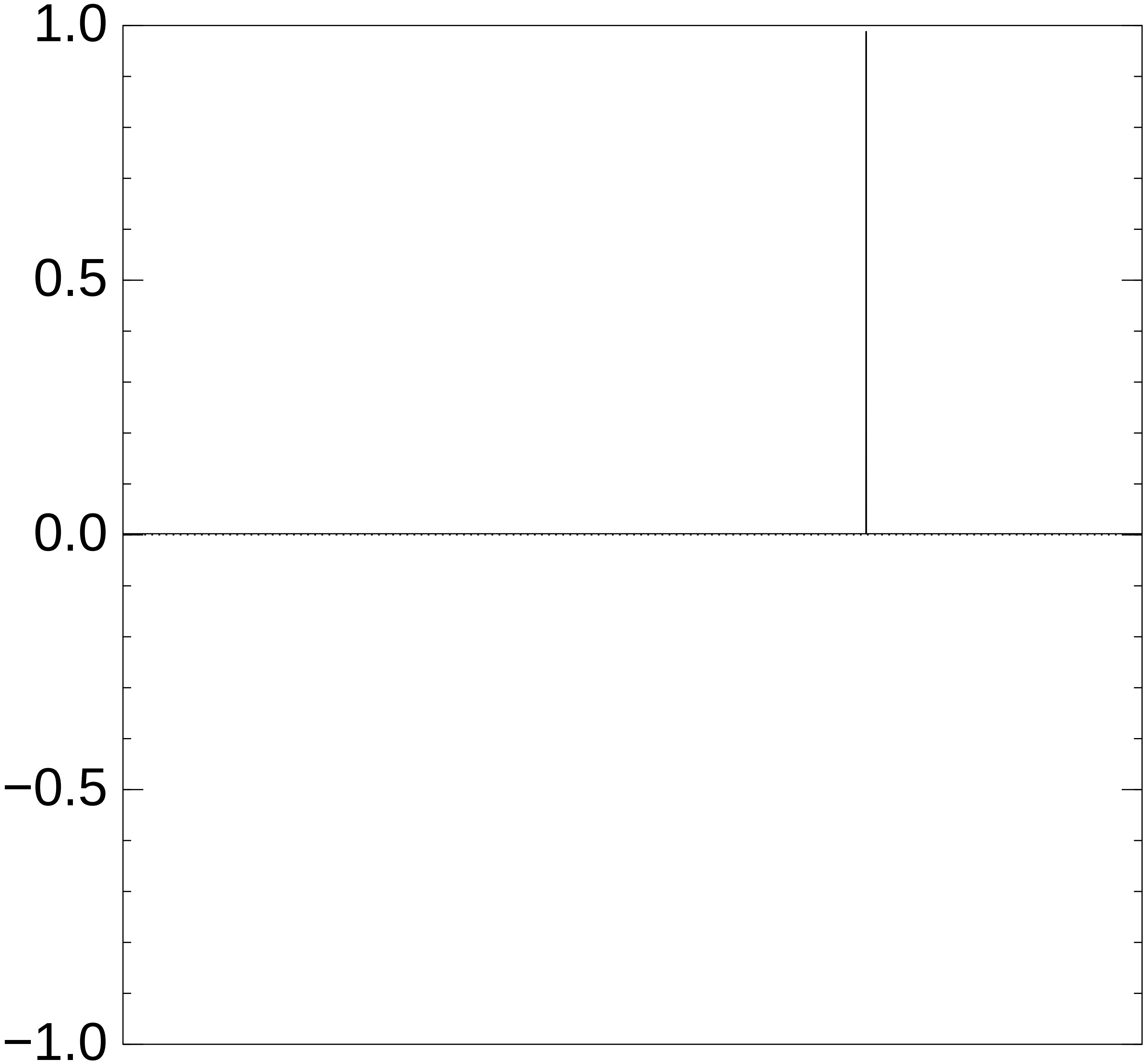
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $40 \times (\text{Step } 1 + \text{Step } 2)$:



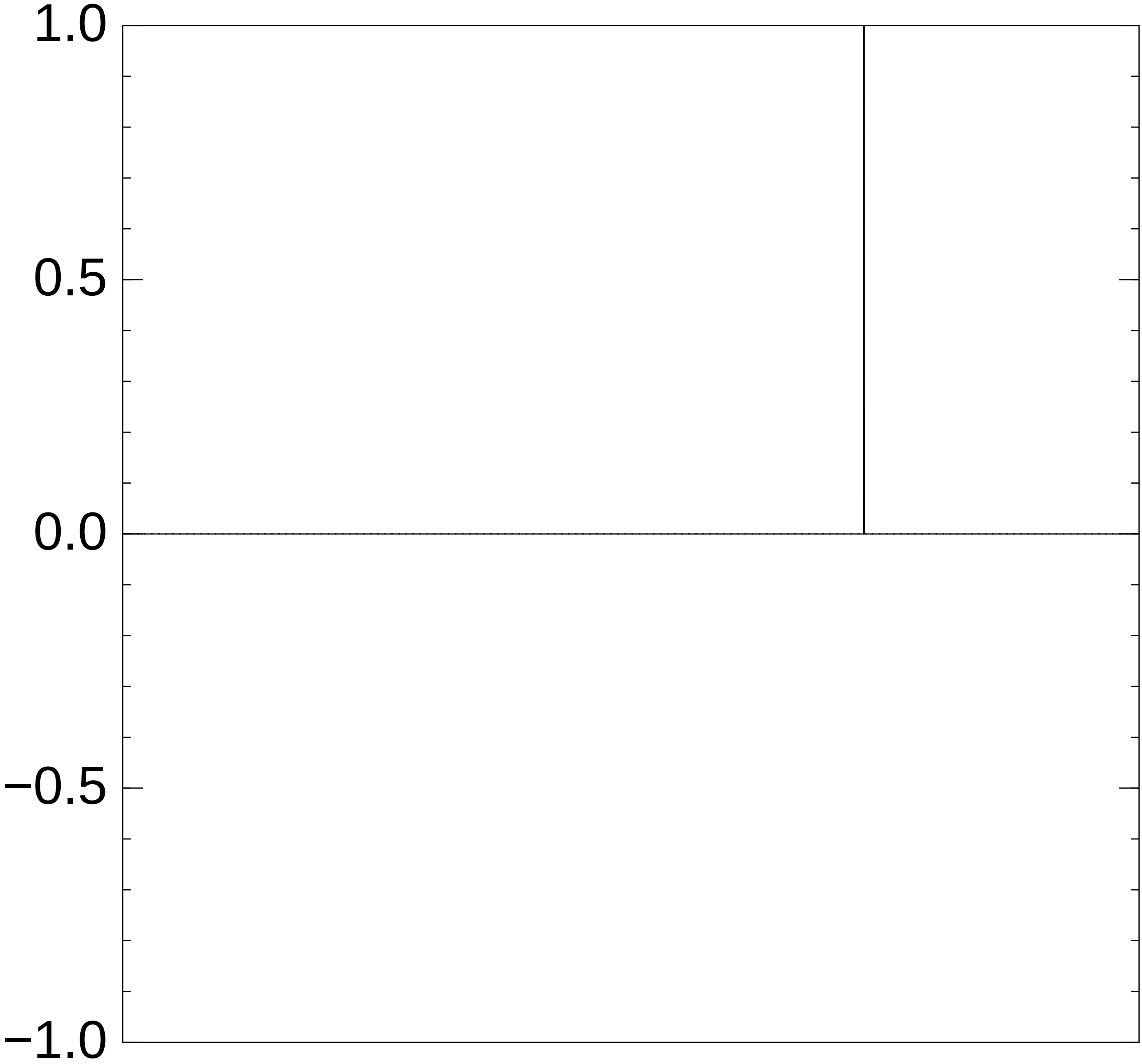
Graph of $J \mapsto a_J$

for 36634 example with $n = 12$

after $45 \times$ (Step $1 +$ Step 2):

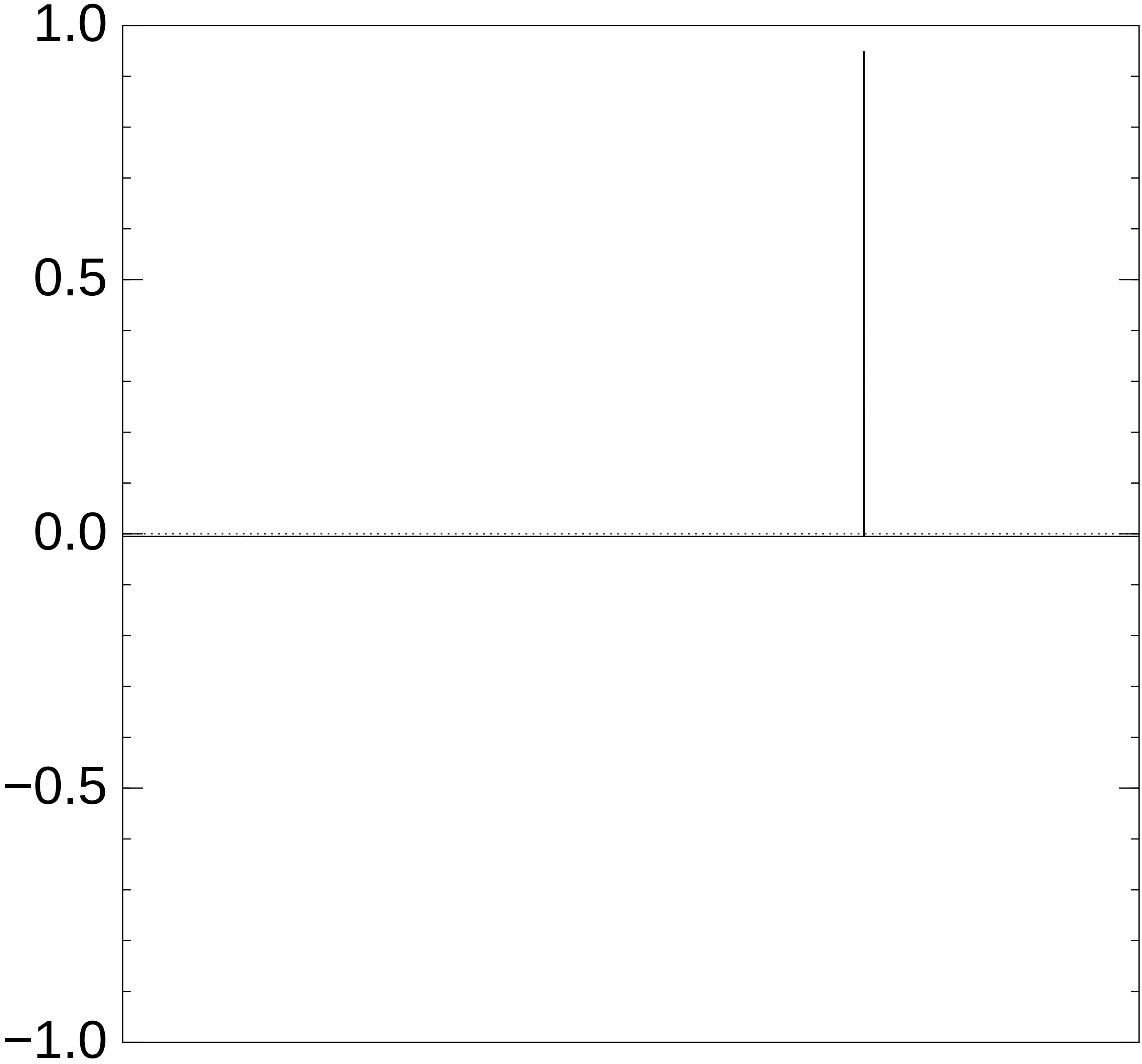


Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $50 \times (\text{Step } 1 + \text{Step } 2)$:

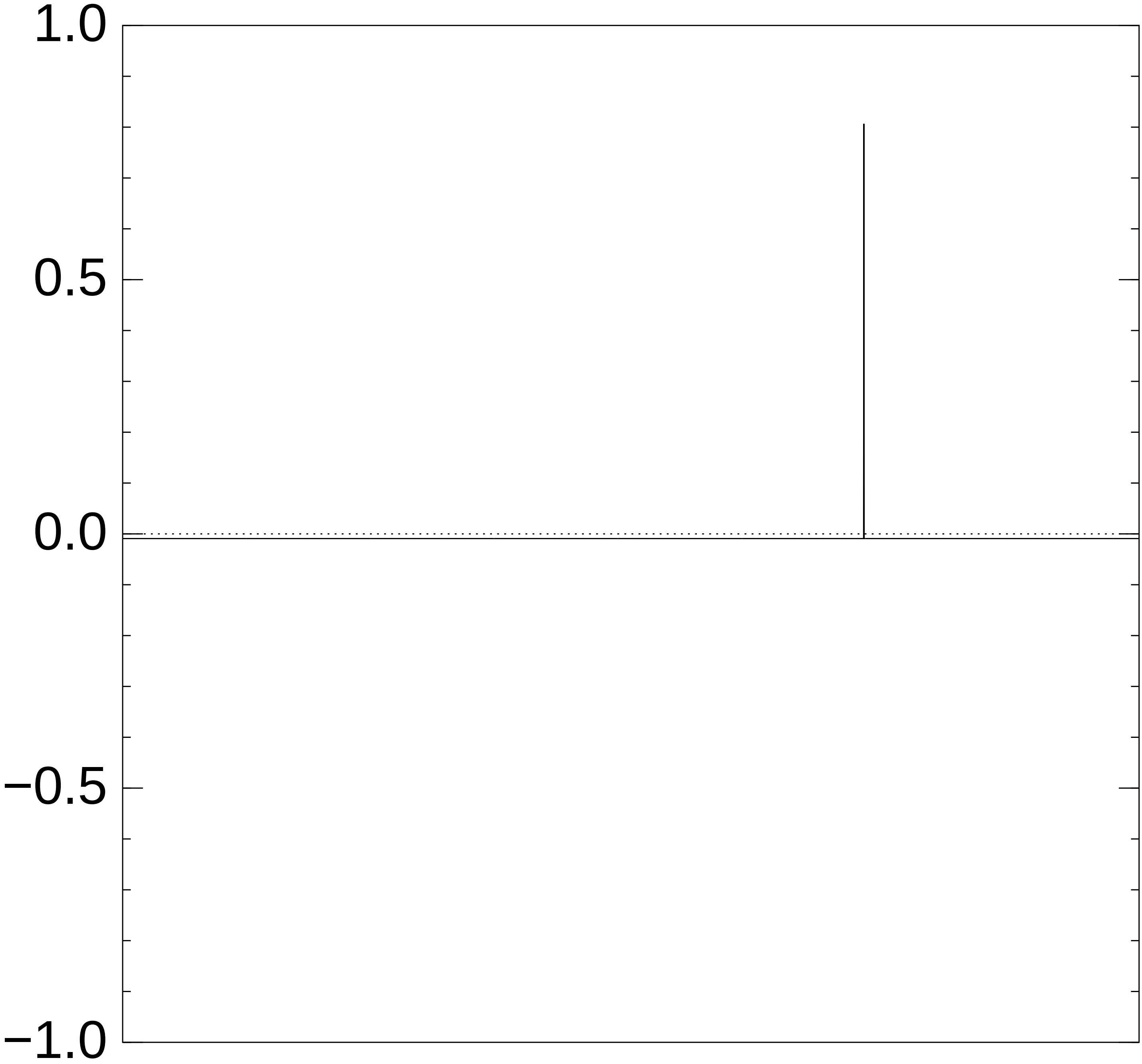


Traditional stopping point.

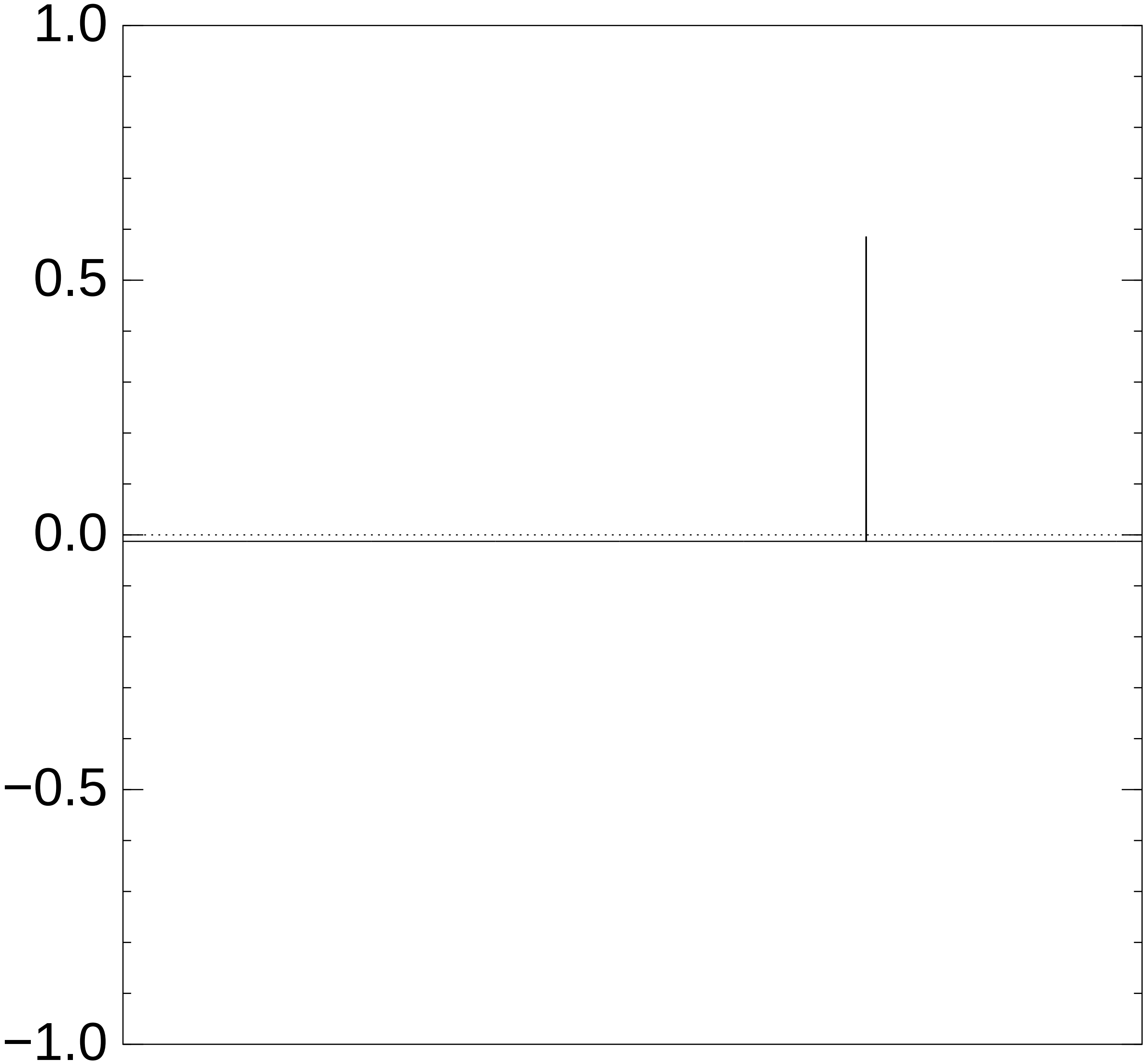
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $60 \times$ (Step $1 +$ Step 2):



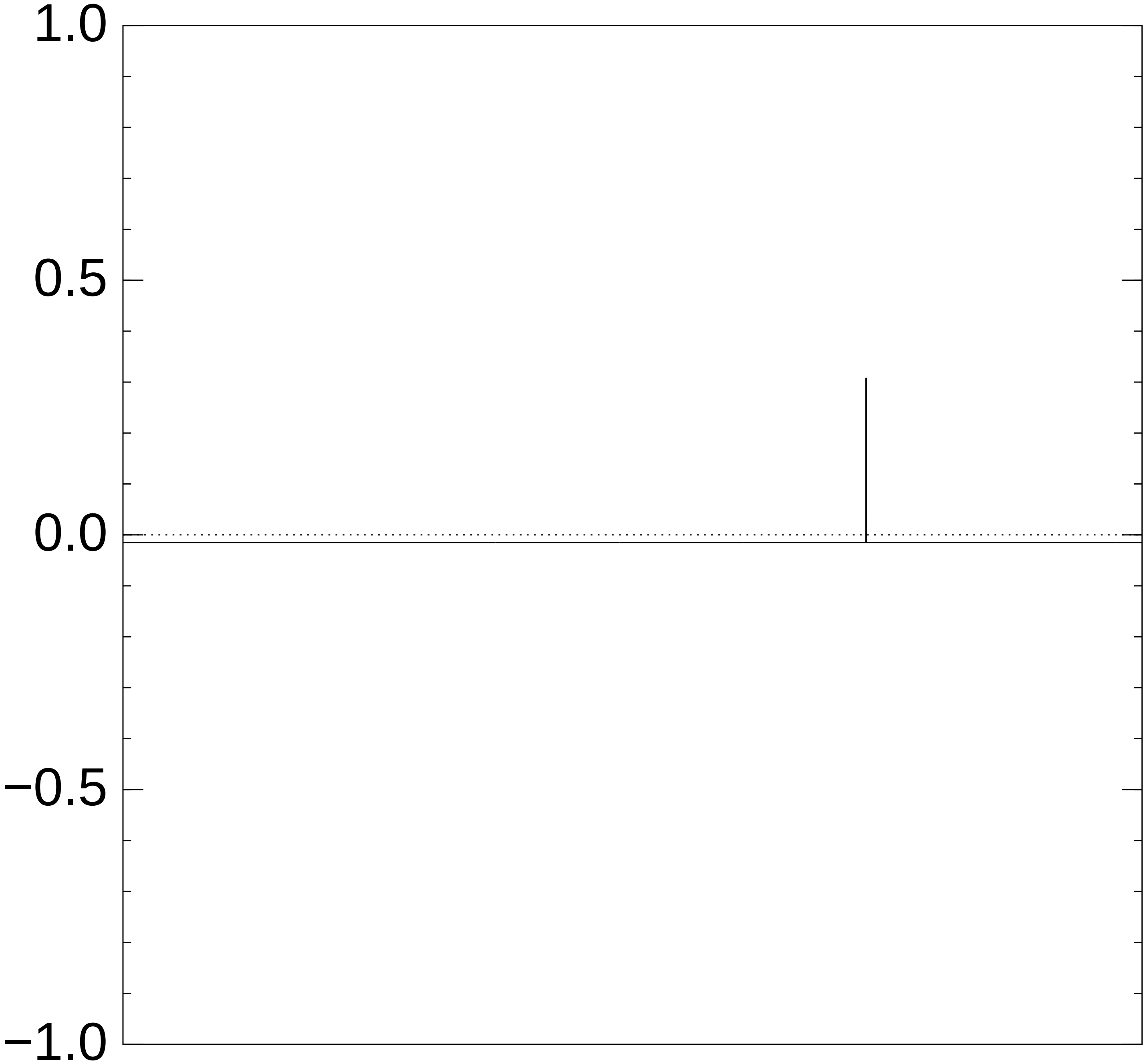
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $70 \times$ (Step $1 +$ Step 2):



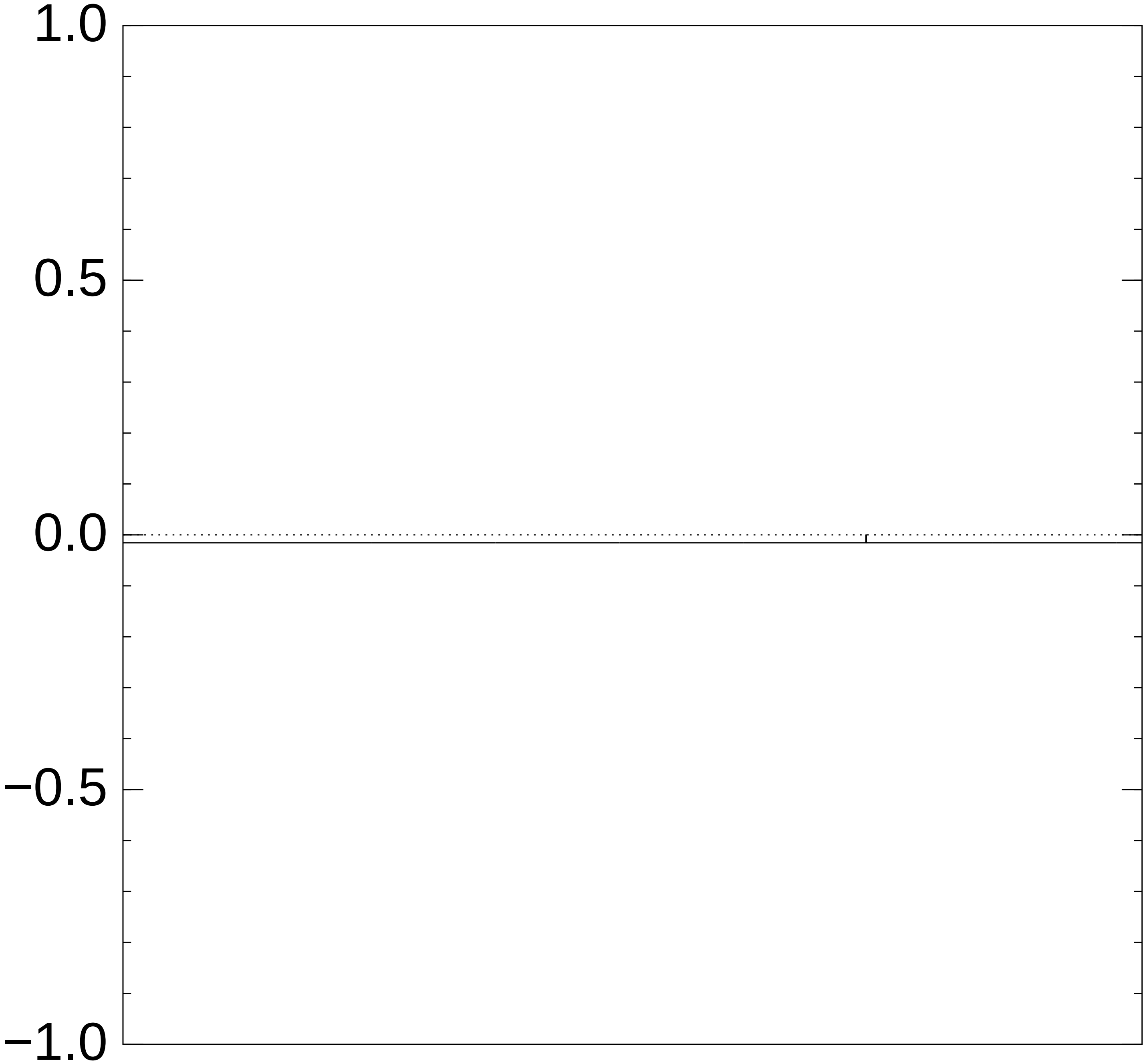
Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $80 \times (\text{Step } 1 + \text{Step } 2)$:



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $90 \times (\text{Step 1} + \text{Step 2})$:



Graph of $J \mapsto a_J$
for 36634 example with $n = 12$
after $100 \times (\text{Step 1} + \text{Step 2})$:



Very bad stopping point.

$J \mapsto a_J$ is completely described
by a vector of two numbers
(with fixed multiplicities):
(1) a_J for roots J;
(2) a_J for non-roots J.

Step 1 $+$ Step 2
act linearly on this vector.

Easily compute eigenvalues
and powers of this linear map
to understand evolution
of state of Grover's algorithm.
$\Rightarrow$ Probability is $\approx$1
after $\approx(\pi/4)2^{0.5n}$ iterations.

Left-right split (0.5)

Don't need quantum computers
to achieve exponent 0.5.

For simplicity assume $n \in 2\mathbf{Z}$.

1974 Horowitz–Sahni:
Sort list of $\Sigma(J_1)$
for all $J_1 \subseteq \{1, \ldots, n/2\}$
and list of $t - \Sigma(J_2)$
for all $J_2 \subseteq \{n/2 + 1, \ldots, n\}$.
Merge to find collisions
$\Sigma(J_1) = t - \Sigma(J_2)$,
i.e., $\Sigma(J_1 \cup J_2) = t$.

Cost $2^{0.5n}$ for sorting, merging.
We assign cost 1 to RAM.

e.g. 36634 as sum of
$(499, 852, 1927, 2535, 3596, 3608,$
$4688, 5989, 6385, 7353, 7650, 9413)$:

Sort the 64 sums
$0, 499, 852, 499+852, \ldots,$
$499+852+1927+\cdots+3608$
and the 64 differences
$36634-0, 36634-4688, \ldots,$
$36634-4688-\cdots-9413$
to see that
$499+852+2535+3608 =$
$36634-5989-6385-7353-9413.$

Moduli (0.5)

For simplicity assume $n \in 4\mathbf{Z}$.

Choose $M \approx 2^{0.25n}$.
Choose $t_1 \in \{0, 1, \ldots, M-1\}$.
Define $t_2 = t - t_1$.

Find all $J_1 \subseteq \{1, \ldots, n/2\}$
such that $\Sigma(J_1) \equiv t_1 \pmod{M}$.
How? Split J_1 as $J_{11} \cup J_{12}$.

Find all $J_2 \subseteq \{n/2+1, \ldots, n\}$
such that $\Sigma(J_2) \equiv t_2 \pmod{M}$.

Sort and merge to find all
collisions $\Sigma(J_1) = t - \Sigma(J_2)$,
i.e., $\Sigma(J_1 \cup J_2) = t$.

Finds J iff $\Sigma(J_1) \equiv t_1$.
There are $\approx 2^{0.25n}$ choices of t_1.
Each choice costs $2^{0.25n}$.
Total cost $2^{0.5n}$.

Not visible in cost metric:
this uses space only $2^{0.25n}$,
assuming typical distribution.

Algorithm has been
introduced at least twice:
2006 Elsenhans–Jahnel;
2010 Howgrave-Graham–Joux.

Different technique
for similar space reduction:
1981 Schroeppel–Shamir.

e.g. $M = 8$, $t = 36634$, $x = (499, 852, 1927, 2535, 3596, 3608, 4688, 5989, 6385, 7353, 7650, 9413)$:

Try each $t_1 \in \{0, 1, \ldots, 7\}$.

In particular try $t_1 = 6$.
There are 12 subsequences of $(499, 852, 1927, 2535, 3596, 3608)$ with sum 6 modulo 8.
There are 6 subsequences of $(4688, 5989, 6385, 7353, 7650, 9413)$ with sum $36634 - 6$ modulo 8.
Sort and merge to find $499 + 852 + 2535 + 3608 = 36634 - 5989 - 6385 - 7353 - 9413$.

Quantum left-right split $(0.333\ldots)$

Cost $2^{n/3}$, imitating
1998 Brassard–Høyer–Tapp:

For simplicity assume $n \in 3\mathbf{Z}$.

Compute $\Sigma(J_1)$ for all
$J_1 \subseteq \{1, 2, \ldots, n/3\}$.
Sort $L = \{\Sigma(J_1)\}$.

Can now efficiently compute
$J_2 \mapsto [t - \Sigma(J_2) \notin L]$
for $J_2 \subseteq \{n/3 + 1, \ldots, n\}$.
Recall: we assign cost 1 to RAM.

Use Grover's method to see
whether this function has a root.

Quantum walk

Unique-collision-finding problem:
Say f has n-bit inputs,
exactly one collision $\{p, q\}$:
i.e., $p \neq q$, $f(p) = f(q)$.
Problem: find this collision.

Cost 2^n: Define S as
the set of n-bit strings.
Compute $f(S)$, sort.

Generalize to cost r,
success probability $\approx(r/2^n)^2$:
Choose a set S of size r.
Compute $f(S)$, sort.

Data structure $D(S)$ capturing
the generalized computation:
the set S; the multiset $f(S)$;
the number of collisions in S.

Very efficient to move from $D(S)$
to $D(T)$ if T is an **adjacent** set:
$\#S = \#T = r$, $\#(S \cap T) = r - 1$.

2003 Ambainis, simplified 2007
Magniez–Nayak–Roland–Santha:
Create superposition of states
$(D(S), D(T))$ with adjacent S, T.
By a quantum walk
find S containing a collision.

How the quantum walk works:

Start from uniform superposition.

Repeat $\approx 0.6 \cdot 2^n/r$ times:

  Negate $a_{S,T}$

    if S contains collision.

  Repeat $\approx 0.7 \cdot \sqrt{r}$ times:

    For each T:

      Diffuse $a_{S,T}$ across all S.

    For each S:

      Diffuse $a_{S,T}$ across all T.

Now high probability

that T contains collision.

Cost $r + 2^n/\sqrt{r}$. Optimize: $2^{2n/3}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 0 negations and 0 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.938; +$
$\Pr[\text{class } (0, 1)] \approx 0.000; +$
$\Pr[\text{class } (1, 0)] \approx 0.000; +$
$\Pr[\text{class } (1, 1)] \approx 0.060; +$
$\Pr[\text{class } (1, 2)] \approx 0.000; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.001; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to $(\#(S \cap \{p,q\}), \#(T \cap \{p,q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 1 negation and 46 diffusions:

$\Pr[\text{class } (0,0)] \approx 0.935; +$
$\Pr[\text{class } (0,1)] \approx 0.000; +$
$\Pr[\text{class } (1,0)] \approx 0.000; -$
$\Pr[\text{class } (1,1)] \approx 0.057; +$
$\Pr[\text{class } (1,2)] \approx 0.000; +$
$\Pr[\text{class } (2,1)] \approx 0.000; -$
$\Pr[\text{class } (2,2)] \approx 0.008; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
2 negations and 92 diffusions:

Pr[class $(0, 0)$] $\approx 0.918; +$
Pr[class $(0, 1)$] $\approx 0.001; +$
Pr[class $(1, 0)$] $\approx 0.000; -$
Pr[class $(1, 1)$] $\approx 0.059; +$
Pr[class $(1, 2)$] $\approx 0.001; +$
Pr[class $(2, 1)$] $\approx 0.000; -$
Pr[class $(2, 2)$] $\approx 0.022; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 3 negations and 138 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.897; +$
$\Pr[\text{class } (0, 1)] \approx 0.001; +$
$\Pr[\text{class } (1, 0)] \approx 0.000; -$
$\Pr[\text{class } (1, 1)] \approx 0.058; +$
$\Pr[\text{class } (1, 2)] \approx 0.002; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.042; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
4 negations and 184 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.873; +$
$\Pr[\text{class } (0, 1)] \approx 0.001; +$
$\Pr[\text{class } (1, 0)] \approx 0.000; -$
$\Pr[\text{class } (1, 1)] \approx 0.054; +$
$\Pr[\text{class } (1, 2)] \approx 0.002; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.070; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
5 negations and 230 diffusions:

$\Pr[\text{class } (0,0)] \approx 0.838; +$
$\Pr[\text{class } (0,1)] \approx 0.001; +$
$\Pr[\text{class } (1,0)] \approx 0.001; -$
$\Pr[\text{class } (1,1)] \approx 0.054; +$
$\Pr[\text{class } (1,2)] \approx 0.003; +$
$\Pr[\text{class } (2,1)] \approx 0.000; +$
$\Pr[\text{class } (2,2)] \approx 0.104; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 6 negations and 276 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.800; +$
$\Pr[\text{class } (0, 1)] \approx 0.001; +$
$\Pr[\text{class } (1, 0)] \approx 0.001; -$
$\Pr[\text{class } (1, 1)] \approx 0.051; +$
$\Pr[\text{class } (1, 2)] \approx 0.006; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.141; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 7 negations and 322 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.758; +$
$\Pr[\text{class } (0, 1)] \approx 0.002; +$
$\Pr[\text{class } (1, 0)] \approx 0.001; -$
$\Pr[\text{class } (1, 1)] \approx 0.047; +$
$\Pr[\text{class } (1, 2)] \approx 0.007; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.184; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 8 negations and 368 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.708; +$
$\Pr[\text{class } (0, 1)] \approx 0.003; +$
$\Pr[\text{class } (1, 0)] \approx 0.001; -$
$\Pr[\text{class } (1, 1)] \approx 0.046; +$
$\Pr[\text{class } (1, 2)] \approx 0.007; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.234; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 9 negations and 414 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.658; +$
$\Pr[\text{class } (0, 1)] \approx 0.003; +$
$\Pr[\text{class } (1, 0)] \approx 0.001; -$
$\Pr[\text{class } (1, 1)] \approx 0.042; +$
$\Pr[\text{class } (1, 2)] \approx 0.009; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.287; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
10 negations and 460 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.606; +$
$\Pr[\text{class } (0, 1)] \approx 0.003; +$
$\Pr[\text{class } (1, 0)] \approx 0.002; -$
$\Pr[\text{class } (1, 1)] \approx 0.037; +$
$\Pr[\text{class } (1, 2)] \approx 0.013; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.338; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to
$(\#(S\cap\{p,q\}),\#(T\cap\{p,q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n=15$, $r=1024$, after
11 negations and 506 diffusions:

$\Pr[\text{class }(0,0)]\approx 0.547; +$
$\Pr[\text{class }(0,1)]\approx 0.004; +$
$\Pr[\text{class }(1,0)]\approx 0.003; -$
$\Pr[\text{class }(1,1)]\approx 0.036; +$
$\Pr[\text{class }(1,2)]\approx 0.015; +$
$\Pr[\text{class }(2,1)]\approx 0.001; +$
$\Pr[\text{class }(2,2)]\approx 0.394; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to $(\#(S\cap\{p,q\}),\#(T\cap\{p,q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n=15$, $r=1024$, after 12 negations and 552 diffusions:

$\Pr[\text{class }(0,0)]\approx 0.491;+$
$\Pr[\text{class }(0,1)]\approx 0.004;+$
$\Pr[\text{class }(1,0)]\approx 0.003;-$
$\Pr[\text{class }(1,1)]\approx 0.032;+$
$\Pr[\text{class }(1,2)]\approx 0.014;+$
$\Pr[\text{class }(2,1)]\approx 0.001;+$
$\Pr[\text{class }(2,2)]\approx 0.455;+$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
13 negations and 598 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.436; +$
$\Pr[\text{class } (0, 1)] \approx 0.005; +$
$\Pr[\text{class } (1, 0)] \approx 0.003; -$
$\Pr[\text{class } (1, 1)] \approx 0.026; +$
$\Pr[\text{class } (1, 2)] \approx 0.017; +$
$\Pr[\text{class } (2, 1)] \approx 0.000; +$
$\Pr[\text{class } (2, 2)] \approx 0.513; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 14 negations and 644 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.377; +$
$\Pr[\text{class } (0, 1)] \approx 0.006; +$
$\Pr[\text{class } (1, 0)] \approx 0.004; -$
$\Pr[\text{class } (1, 1)] \approx 0.025; +$
$\Pr[\text{class } (1, 2)] \approx 0.022; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.566; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to
$(\#(S \cap \{p,q\}), \#(T \cap \{p,q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
15 negations and 690 diffusions:

$\Pr[\text{class } (0,0)] \approx 0.322; +$
$\Pr[\text{class } (0,1)] \approx 0.005; +$
$\Pr[\text{class } (1,0)] \approx 0.004; -$
$\Pr[\text{class } (1,1)] \approx 0.021; +$
$\Pr[\text{class } (1,2)] \approx 0.023; +$
$\Pr[\text{class } (2,1)] \approx 0.001; +$
$\Pr[\text{class } (2,2)] \approx 0.623; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 16 negations and 736 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.270; +$
$\Pr[\text{class } (0, 1)] \approx 0.006; +$
$\Pr[\text{class } (1, 0)] \approx 0.005; -$
$\Pr[\text{class } (1, 1)] \approx 0.017; +$
$\Pr[\text{class } (1, 2)] \approx 0.022; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.680; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 17 negations and 782 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.218; +$
$\Pr[\text{class } (0, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 0)] \approx 0.005; -$
$\Pr[\text{class } (1, 1)] \approx 0.015; +$
$\Pr[\text{class } (1, 2)] \approx 0.024; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.730; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 18 negations and 828 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.172; +$
$\Pr[\text{class } (0, 1)] \approx 0.006; +$
$\Pr[\text{class } (1, 0)] \approx 0.005; -$
$\Pr[\text{class } (1, 1)] \approx 0.011; +$
$\Pr[\text{class } (1, 2)] \approx 0.029; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.775; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
19 negations and 874 diffusions:

$\Pr[\text{class } (0,0)] \approx 0.131; +$
$\Pr[\text{class } (0,1)] \approx 0.007; +$
$\Pr[\text{class } (1,0)] \approx 0.006; -$
$\Pr[\text{class } (1,1)] \approx 0.008; +$
$\Pr[\text{class } (1,2)] \approx 0.030; +$
$\Pr[\text{class } (2,1)] \approx 0.002; +$
$\Pr[\text{class } (2,2)] \approx 0.816; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 20 negations and 920 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.093; +$
$\Pr[\text{class } (0, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 0)] \approx 0.007; -$
$\Pr[\text{class } (1, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 2)] \approx 0.027; +$
$\Pr[\text{class } (2, 1)] \approx 0.002; +$
$\Pr[\text{class } (2, 2)] \approx 0.857; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to $(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$; reduce a to low-dim vector. Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after 21 negations and 966 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.062; +$
$\Pr[\text{class } (0, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 0)] \approx 0.006; -$
$\Pr[\text{class } (1, 1)] \approx 0.004; +$
$\Pr[\text{class } (1, 2)] \approx 0.030; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.890; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
22 negations and 1012 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.037; +$
$\Pr[\text{class } (0, 1)] \approx 0.008; +$
$\Pr[\text{class } (1, 0)] \approx 0.007; -$
$\Pr[\text{class } (1, 1)] \approx 0.002; +$
$\Pr[\text{class } (1, 2)] \approx 0.034; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.910; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to
$(\#(S \cap \{p,q\}), \#(T \cap \{p,q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
23 negations and 1058 diffusions:

$\Pr[\text{class } (0,0)] \approx 0.017; +$
$\Pr[\text{class } (0,1)] \approx 0.008; +$
$\Pr[\text{class } (1,0)] \approx 0.007; -$
$\Pr[\text{class } (1,1)] \approx 0.002; +$
$\Pr[\text{class } (1,2)] \approx 0.034; +$
$\Pr[\text{class } (2,1)] \approx 0.002; +$
$\Pr[\text{class } (2,2)] \approx 0.930; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
24 negations and 1104 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.005; +$
$\Pr[\text{class } (0, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 0)] \approx 0.007; -$
$\Pr[\text{class } (1, 1)] \approx 0.000; +$
$\Pr[\text{class } (1, 2)] \approx 0.030; +$
$\Pr[\text{class } (2, 1)] \approx 0.002; +$
$\Pr[\text{class } (2, 2)] \approx 0.948; +$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
25 negations and 1150 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.000; +$
$\Pr[\text{class } (0, 1)] \approx 0.008; +$
$\Pr[\text{class } (1, 0)] \approx 0.008; -$
$\Pr[\text{class } (1, 1)] \approx 0.000; +$
$\Pr[\text{class } (1, 2)] \approx 0.031; +$
$\Pr[\text{class } (2, 1)] \approx 0.001; +$
$\Pr[\text{class } (2, 2)] \approx 0.952; +$

Right column is sign of $a_{S,T}$.

Classify (S,T) according to
$(\#(S\cap\{p,q\}),\#(T\cap\{p,q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n=15$, $r=1024$, after
26 negations and 1196 diffusions:

$\Pr[\text{class }(0,0)]\approx 0.002;-$
$\Pr[\text{class }(0,1)]\approx 0.008;+$
$\Pr[\text{class }(1,0)]\approx 0.008;-$
$\Pr[\text{class }(1,1)]\approx 0.000;-$
$\Pr[\text{class }(1,2)]\approx 0.035;+$
$\Pr[\text{class }(2,1)]\approx 0.002;+$
$\Pr[\text{class }(2,2)]\approx 0.945;+$

Right column is sign of $a_{S,T}$.

Classify (S, T) according to
$(\#(S \cap \{p, q\}), \#(T \cap \{p, q\}))$;
reduce a to low-dim vector.
Analyze evolution of this vector.

e.g. $n = 15$, $r = 1024$, after
27 negations and 1242 diffusions:

$\Pr[\text{class } (0, 0)] \approx 0.011; -$
$\Pr[\text{class } (0, 1)] \approx 0.007; +$
$\Pr[\text{class } (1, 0)] \approx 0.007; -$
$\Pr[\text{class } (1, 1)] \approx 0.001; -$
$\Pr[\text{class } (1, 2)] \approx 0.034; +$
$\Pr[\text{class } (2, 1)] \approx 0.003; +$
$\Pr[\text{class } (2, 2)] \approx 0.938; +$

Right column is sign of $a_{S,T}$.

Subset-sum walk (0.333 . . .)

Consider f defined by
$f(1, J_1) = \Sigma(J_1)$
for $J_1 \subseteq \{1, \ldots, n/2\}$;
$f(2, J_2) = t - \Sigma(J_2)$
for $J_2 \subseteq \{n/2 + 1, \ldots, n\}$.

Good chance of unique
collision $\Sigma(J_1) = t - \Sigma(J_2)$.

$n/2 + 1$ bits of input,
so quantum walk costs $2^{n/3}$.

Easily tweak quantum walk
to handle more collisions,
ignore $\Sigma(J_1) = \Sigma(J_1')$, etc.

Generalized moduli

Choose M, t_1, r with $M \approx r$.
(Original moduli algorithm
is the special case $r = 2^{n/4}$.)

Take set S_{11}, $\#S_{11} = r$, where
$J_{11} \in S_{11} \Rightarrow J_{11} \subseteq \{1, \ldots, n/4\}$.
(Original algorithm: S_{11} is the set
of *all* $J_{11} \subseteq \{1, \ldots, n/4\}$.)
Compute $\Sigma(J_{11}) \bmod M$
for each $J_{11} \in S_{11}$.

Similarly take a set S_{12} of r
subsets of $\{n/4 + 1, \ldots, n/2\}$.
Compute $t_1 - \Sigma(J_{12}) \bmod M$
for each $J_{12} \in S_{12}$.

Find all collisions

$\Sigma(J_{11}) \equiv t_1 - \Sigma(J_{12})$,

i.e., $\Sigma(J_1) \equiv t_1 \pmod M$

where $J_1 = J_{11} \cup J_{12}$.

Compute each $\Sigma(J_1)$.

Similarly S_{21}, $S_{22} \Rightarrow$

list of J_2 with $\Sigma(J_2) \equiv t - t_1$

$\Rightarrow$ each $t - \Sigma(J_2)$.

Find collisions $\Sigma(J_1) = t - \Sigma(J_2)$.

Success probability $r^4/2^n$

at finding any particular J with

$\Sigma(J) = t$, $\Sigma(J_1) \equiv t_1 \pmod M$.

Assuming typical distribution:

cost r, since $M \approx r$.

Quantum moduli (0.3)

Capture execution of
generalized moduli algorithm
as data structure
$D(S_{11}, S_{12}, S_{21}, S_{22})$.
Easy to move
from S_{ij} to adjacent T_{ij}.

Convert into quantum walk:
cost $r + \sqrt{r}2^{n/2}/r^2$.
$2^{0.2n}$ for $r \approx 2^{0.2n}$.

Use "amplitude amplification"
to search for correct t_1.
Total cost $2^{0.3n}$.

Quantum reps (0.241 . . .)

Central result of the paper:
Combine quantum walk
with "representations" idea of
2010 Howgrave-Graham–Joux.
Subset-sum exponent 0.241 . . .;
new record.

Lower-level improvement:
Ambainis uses ad-hoc
"combination of a hash table
and a skip list" to ensure
history-independence.
We use radix trees.
Much easier, presumably faster.