Randomized OBDDs for the Most Significant Bit of Multiplication Need Exponential Size

Beate Bollig and Marc Gillé

LS2 Informatik, TU Dortmund
Germany

SOFSEM 2011

Outline

- Introduction and result
  - Integer multiplication
  - Randomized OBDDs

Outline

- Introduction and result
  - Integer multiplication
  - Randomized OBDDs
- Randomized OBDDs for integer multiplication need exponential size
  - Proof ingredients for the exponential lower bound

Outline

- Introduction and result
  - Integer multiplication
  - Randomized OBDDs
- Randomized OBDDs for integer multiplication need exponential size
  - Proof ingredients for the exponential lower bound
  - The rectangular reduction from the greater than function to integer multiplication

Outline

- Introduction and result
  - Integer multiplication
  - Randomized OBDDs
- Randomized OBDDs for integer multiplication need exponential size
  - Proof ingredients for the exponential lower bound
  - The rectangular reduction from the greater than function to integer multiplication
- Concluding remarks

Integer multiplication

Integer multiplication is one of the most important functions in computer science

$\longrightarrow$ a lot of effort in

- designing efficient algorithms and small circuits and
- determining its complexity

Integer multiplication

Integer multiplication is one of the most important functions in computer science

$\rightarrow$ a lot of effort in

- designing efficient algorithms and small circuits and
- determining its complexity

Definition

The Boolean function $\mathrm{MUL}_{i,n} \in B_{2n}$ maps two n-bit integers $x = x_{n-1} \dots x_0$ and $y = y_{n-1} \dots y_0$ to the ith bit of their binary product $z_{2n-1} \dots z_0$, i.e., $\mathrm{MUL}_{i,n}(x, y) = z_i$, where x_0, y_0, z_0 denote the least significant bits.

$\mathrm{MUL}_{n-1,n}$: *middle bit of integer multiplication*
$\mathrm{MUL}_{2n-1,n}$: *most significant bit of integer multiplication*

Ordered Binary Decision Diagrams (OBDDs)

In many applications data structures for Boolean functions are necessary:

- circuit verification
- model checking
- even in graph algorithms ...

Ordered Binary Decision Diagrams (OBDDs)

In many applications data structures for Boolean functions are necessary:

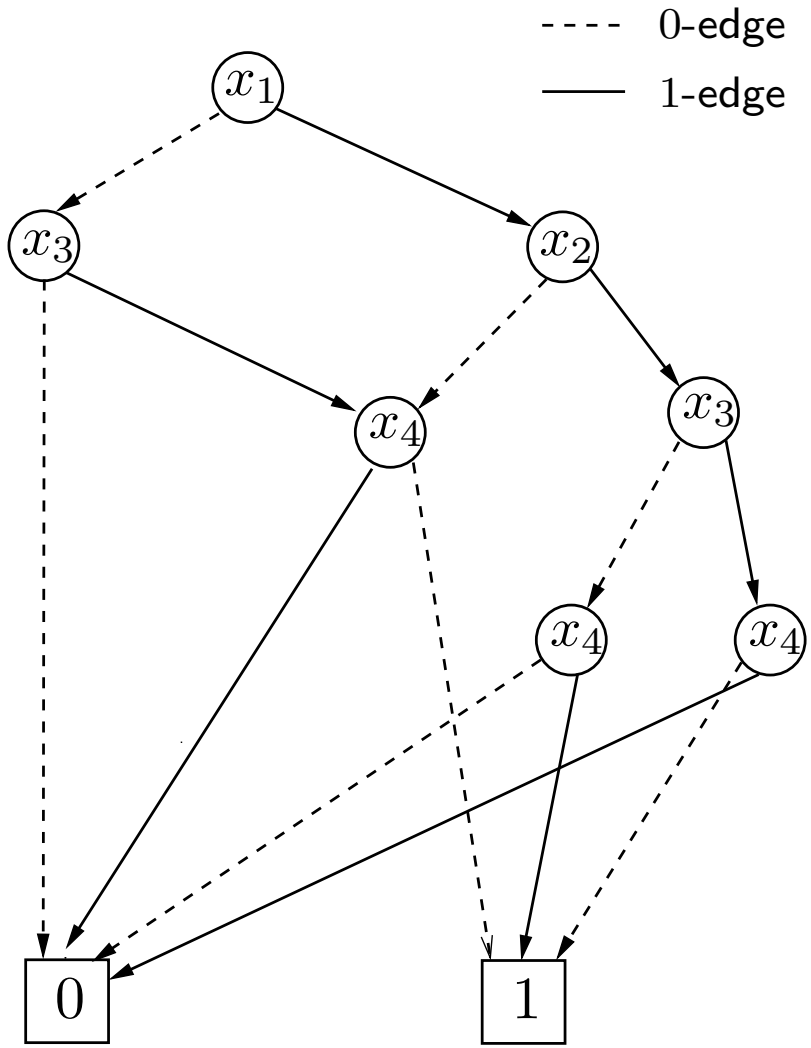
- circuit verification
- model checking
- even in graph algorithms ...

Ordered Binary Decision Diagrams (OBDDs) [Bryant (1986)]:

- support efficiently all fundamental operations on Boolean functions
- are one of the state-of-the art data structures for Boolean functions

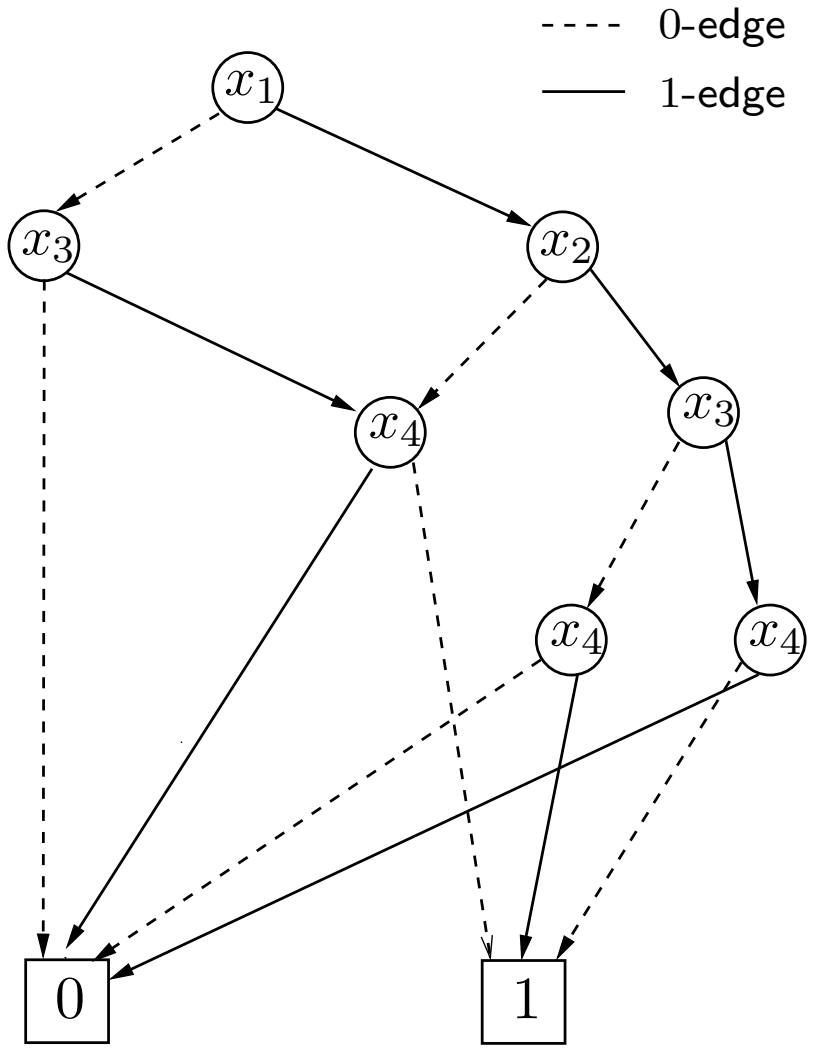
Ordered Binary Decision Diagrams (OBDDs)

- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1



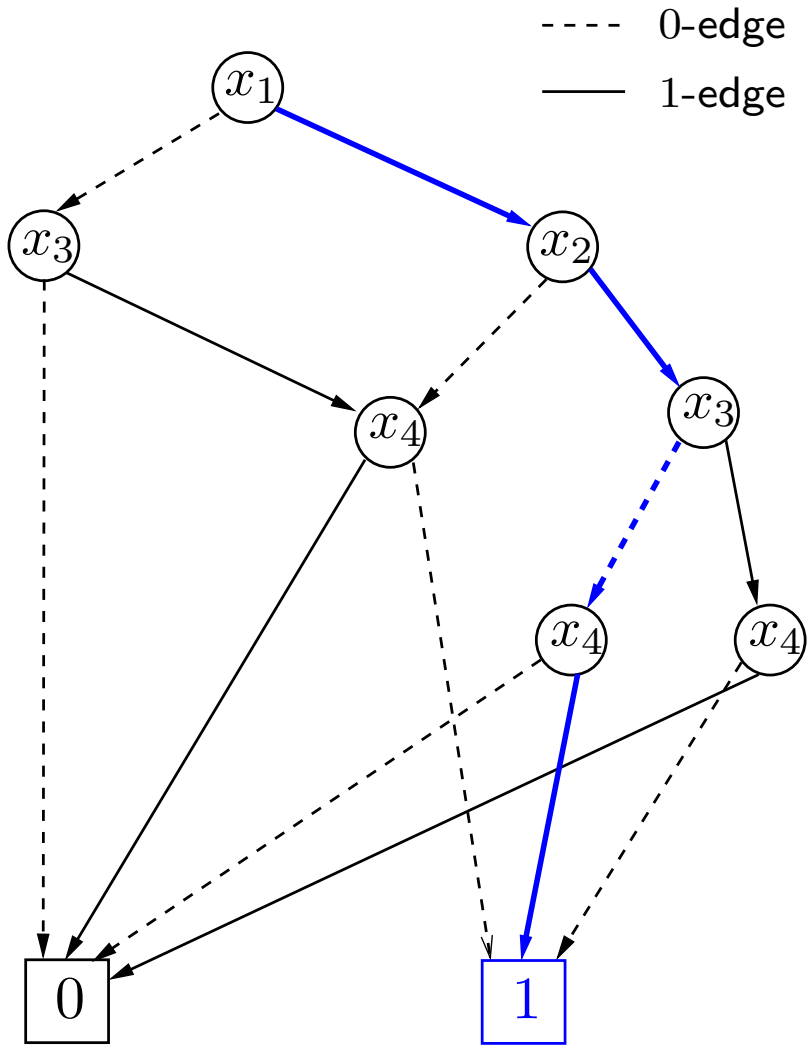
Ordered Binary Decision Diagrams (OBDDs)

- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1
- variable ordering π on each path



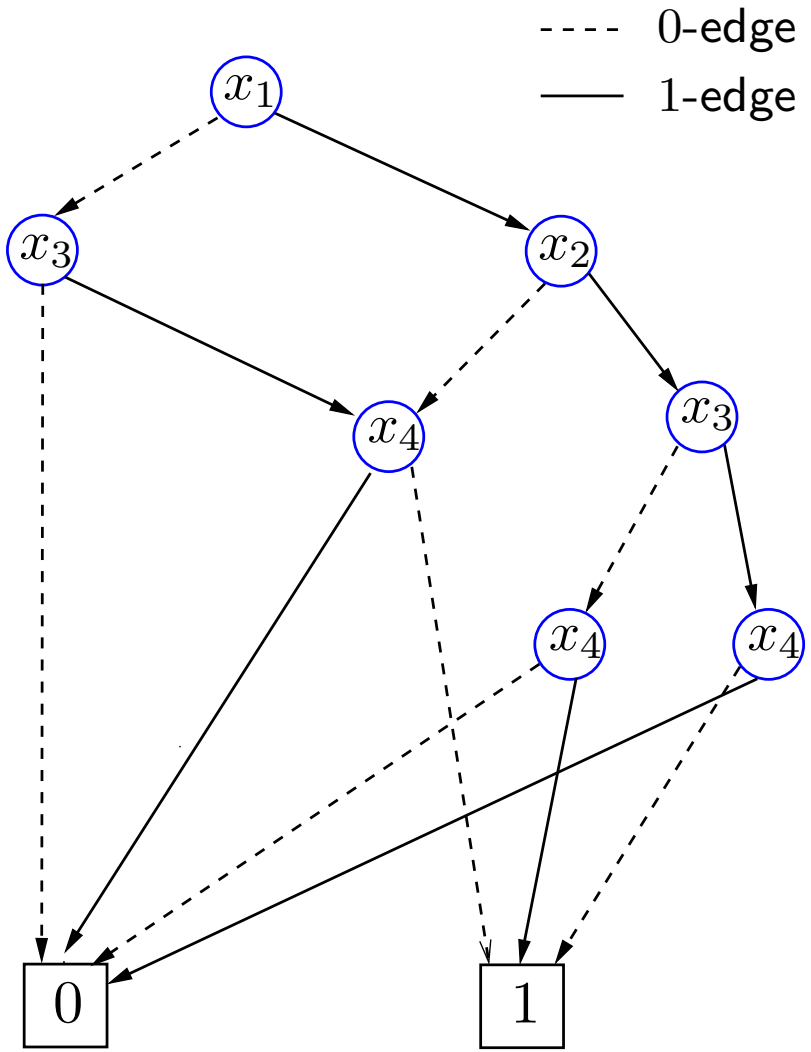
Ordered Binary Decision Diagrams (OBDDs)

- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1
- variable ordering π on each path
- $f(b) = c \;:\Leftrightarrow$
  computation path for b leads to c-sink



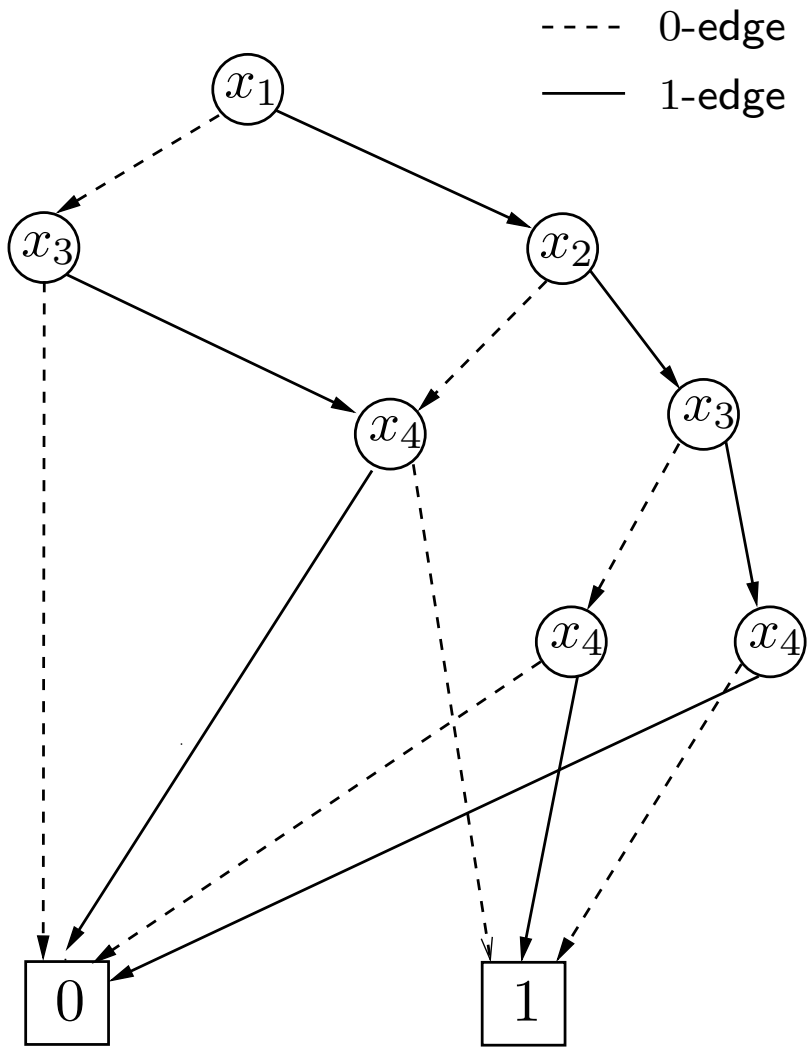
Ordered Binary Decision Diagrams (OBDDs)

- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1
- variable ordering π on each path
- $f(b) = c \;:\Leftrightarrow$
  computation path for b leads to c-sink
- size of a π-OBDD: # nodes



Ordered Binary Decision Diagrams (OBDDs)

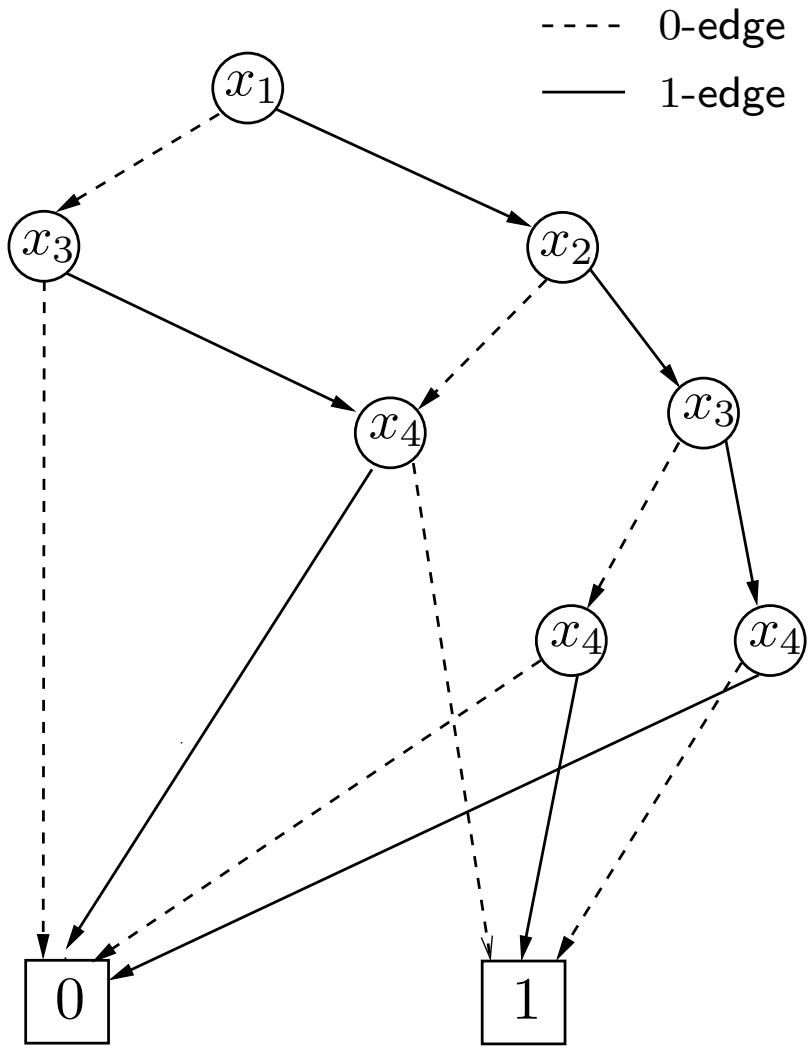
- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1
- variable ordering π on each path
- $f(b) = c \;:\Leftrightarrow$
  computation path for b leads to c-sink
- size of a π-OBDD: # nodes
- OBDD(f): minimal size of an OBDD for f



Ordered Binary Decision Diagrams (OBDDs)

- directed acyclic graph
- decision nodes:
  – marked by a Boolean variable
  – outgoing 0- and 1-edge
- one source and two sinks: 0 and 1
- variable ordering π on each path
- $f(b) = c \;:\Leftrightarrow$
  computation path for b leads to c-sink

The size of an OBDD for a function f depends on the chosen variable ordering π.



Randomized OBDDs

Randomized OBDDs can be defined like randomized algorithms for decision problems:

Definition

A randomized node is an unlabeled node with two outgoing edges. A randomized OBDD G is an OBDD with additional randomized nodes. The random computation path for an input b is defined as follows:

- at decision nodes labeled by x_i the outgoing b_i-edge is chosen,
- at randomized nodes each outgoing edge is chosen independently from all other random decisions with probability $1/2$.

G represents a function $f \in B_n$ with two-sided ε-bounded error, $0 \leq \varepsilon < 1/2$, if Prob$(G(b) \neq f(b)) \leq \varepsilon$ for all inputs b.

Integer multiplication and (randomized) OBDDs

$\mathrm{OBDD}(\mathrm{MUL}_{n-1,n}) = 2^{\Omega(n)}$ [Bryant (1991)]
$\mathrm{OBDD}(\mathrm{MUL}_{2n-1,n}) = 2^{\Omega(n)}$ [B. (2008)]

Integer multiplication and (randomized) OBDDs

OBDD($\mathrm{MUL}_{n-1,n}$) $= 2^{\Omega(n)}$ [Bryant (1991)]
OBDD($\mathrm{MUL}_{2n-1,n}$) $= 2^{\Omega(n)}$ [B. (2008)]

Probabilistic methods are useful in almost all areas of computer science. Does randomization help to represent integer multiplication in smaller size?

The size of randomized OBDDs with two-sided bounded error for $\mathrm{MUL}_{n-1,n}$ is $2^{\Omega(n/\log n)}$. [Ablayev, Karpinski (2003)]

Integer multiplication and (randomized) OBDDs

OBDD($\mathrm{MUL}_{n-1,n}$) $= 2^{\Omega(n)}$ [Bryant (1991)]
OBDD($\mathrm{MUL}_{2n-1,n}$) $= 2^{\Omega(n)}$ [B. (2008)]

Probabilistic methods are useful in almost all areas of computer science. Does randomization help to represent integer multiplication in smaller size?

The size of randomized OBDDs with two-sided bounded error for $\mathrm{MUL}_{n-1,n}$ is $2^{\Omega(n/\log n)}$. [Ablayev, Karpinski (2003)]

New: The size of randomized OBDDs with two-sided bounded error for $\mathrm{MUL}_{2n-1,n}$ is $2^{\Omega(n)}$.

By-product: The size of randomized OBDDs with two-sided bounded error for $\mathrm{MUL}_{n-1,n}$ is $2^{\Omega(n)}$.

One-round communication complexity is a standard technique to obtain lower bounds on the size of OBDDs:

Theorem

Let $f : \{0,1\}^{|X_A|} \times \{0,1\}^{|X_B|} \to \{0,1\}$ *and* G_f *be an arbitrary randomized* OBDD *representing* f *with respect to a variable ordering where the variables in* X_A *are before the variables in* X_B*. Then* $R(f) \leq \lceil \log |G_f| \rceil$ *for the randomized one-round communication complexity* $R(f)$*.*

One-round communication complexity is a standard technique to obtain lower bounds on the size of OBDDs:

Theorem

Let $f : \{0,1\}^{|X_A|} \times \{0,1\}^{|X_B|} \to \{0,1\}$ *and* G_f *be an arbitrary randomized* OBDD *representing* f *with respect to a variable ordering where the variables in* X_A *are before the variables in* X_B. *Then* $R(f) \leq \lceil \log |G_f| \rceil$ *for the randomized one-round communication complexity* $R(f)$.

Definition

Let $\mathsf{GT}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be defined by $\mathsf{GT}_n(a,b) = 1$ iff $[a]_0^{n-1} > [b]_0^{n-1}$.

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

Well-known: $R(\mathsf{GT}_n) = \Theta(n)$ [Miltersen et al (1998)]

Key idea of our lower bound proof

A rectangular reduction

For every variable ordering π:
π-OBDD G for $\mathsf{MUL}_{2n-1,n}(x,y) \longrightarrow \pi$-OBDD for $\overline{\mathsf{GT}}_{n'}(a,b)$,
$n' = \Theta(n)$, where all a-variables are before the b-variables in π

Key idea of our lower bound proof

A rectangular reduction

For every variable ordering π:
π-OBDD G for $\mathsf{MUL}_{2n-1,n}(x,y) \rightarrow \pi$-OBDD for $\overline{\mathsf{GT}}_{n'}(a,b)$,
$n' = \Theta(n)$, where all a-variables are before the b-variables in π

$\rightarrow R(\overline{\mathsf{GT}}_n) \leq \lceil \log |G| \rceil$

Well-known: $R(\overline{\mathsf{GT}}_n) = \Theta(n)$

$\rightarrow$ The size of randomized OBDDs with two-sided bounded error for $\mathsf{MUL}_{2n-1,n}$ is $2^{\Omega(n)}$.

To be more precise...

Fact

- $a = 2^{n-1} + \ell\ 2^{n/3},\ 0 < \ell < 2^{n/3-1}$
- $\min\{b \mid a \cdot b \geq 2^{2n-1}\} =$
  $2^n - \ell\ 2^{n/3+1} + \left\lceil \ell^2\ 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil$

To be more precise...

Fact

- $a = 2^{n-1} + \ell\ 2^{n/3},\ 0 < \ell < 2^{n/3-1}$
- $\min\{b \mid a \cdot b \geq 2^{2n-1}\} =$
  $2^n - \ell\ 2^{n/3+1} + \left\lceil \ell^2\ 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil$

$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3}$

- $[y]_{n/3}^{n-1} > (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$: $x \cdot y \geq 2^{2n-1}$
- $[y]_{n/3}^{n-1} = (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$:
  $([y]_0^{n/3-1} \geq \left\lceil \ell^2 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil \leftrightarrow x \cdot y \geq 2^{2n-1})$

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

Closer look at ℓ^2 and some replacements I

If $\ell := u2^m + w$, then $\ell^2 = u^2 2^{2m} + uw2^{m+1} + w^2$.

Closer look at ℓ^2 and some replacements I

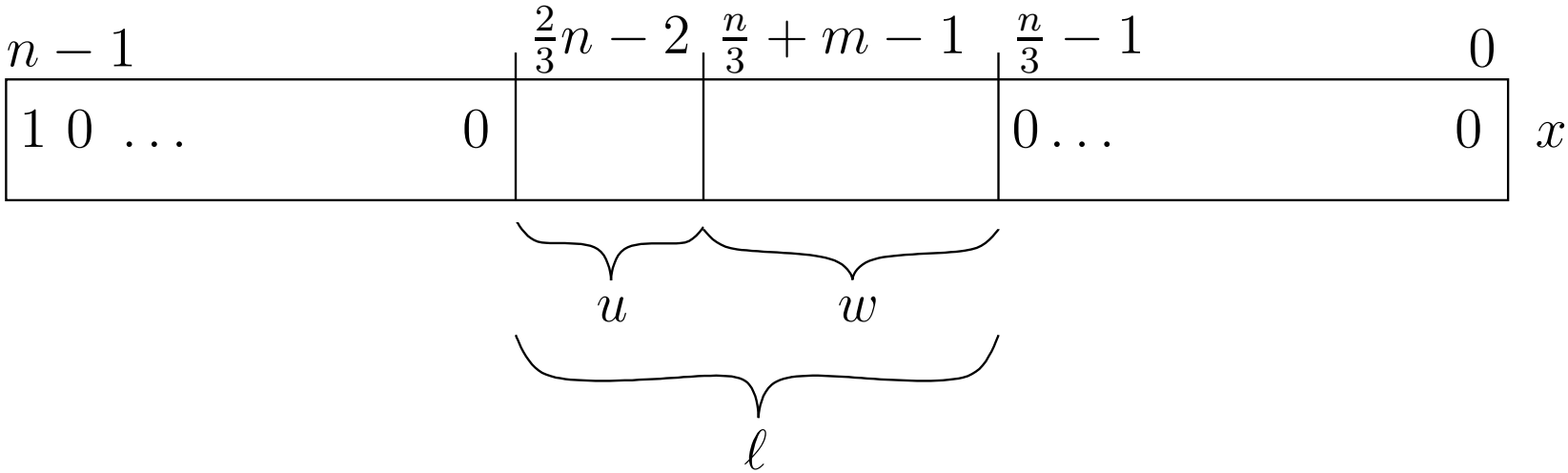
If $\ell := u2^m + w$, then $\ell^2 = u^2 2^{2m} + uw2^{m+1} + w^2$.

Here: $u < 2^{(7/8)m}$ and $w < 2^m$ and $m := (8/45)n - 8/15$

Closer look at ℓ^2 and some replacements I

If $\ell := u2^m + w$, then $\ell^2 = u^2 2^{2m} + uw2^{m+1} + w^2$.

Here: $u < 2^{(7/8)m}$ and $w < 2^m$ and $m := (8/45)n - 8/15$



$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3}$

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

Closer look at ℓ^2 and some replacements II

$$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3} \text{ and } [y]_{n/3}^{n-1} = (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$$

$$[y]_0^{n/3-1} \geq \left\lceil \ell^2 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil \leftrightarrow x \cdot y \geq 2^{2n-1}$$

$$\ell = u2^m + w \text{ and } \ell^2 = u^2 2^{2m} + uw2^{m+1} + w^2$$

Closer look at ℓ^2 and some replacements II

$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3}$ and $[y]_{n/3}^{n-1} = (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$

$[y]_0^{n/3-1} \geq \left\lceil \ell^2 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil \leftrightarrow x \cdot y \geq 2^{2n-1}$

$\ell = u2^m + w$ and $\ell^2 = u^2 2^{2m} + uw2^{m+1} + w^2$

Ideas:

- choose some of the assignments to the y-variables such that we get rid of the influence of w^2 and $-\frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}}$
  $\rightarrow [y]_{2m+1-n/3+2}^{n/3-1} \geq u^2 2^{-1} + uw$ div $2^m \leftrightarrow x \cdot y \geq 2^{2n-1}$
- u power of 2 $\rightarrow$ uw is equal to w shifted to the left

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

More details...

A case inspection:

- define cut in π after $m/2$ of the m variables in $\{x_{n/3+m/2}, \ldots, x_{n/3+m-1}, y_{2m+1-n/3+2}, \ldots, y_{5m/2-n/3+2}\}$

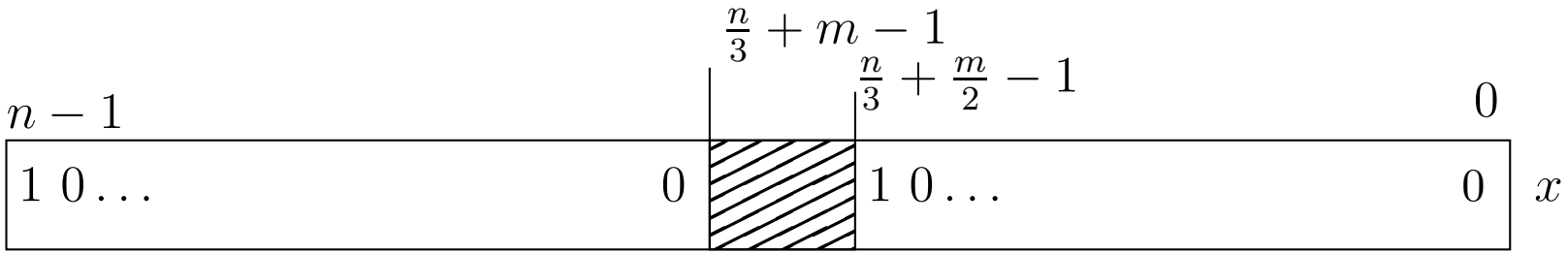
More details...

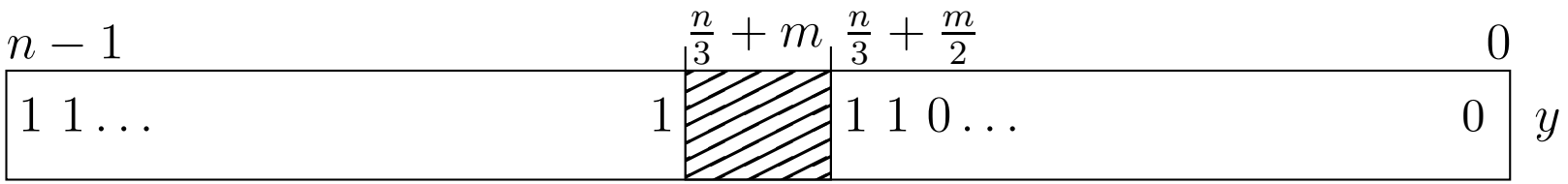
A case inspection:

- define cut in π after $m/2$ of the m variables in $\{x_{n/3+m/2}, \ldots, x_{n/3+m-1}, y_{2m+1-n/3+2}, \ldots, y_{5m/2-n/3+2}\}$
- counting arguments
  $\rightarrow \exists\ d$: at least $m/8$ pairs $(x_{n/3+i}, y_{m+1+i+d-n/3+2})$ separated in π with respect to the cut
- I set of indices i, $m/2 \leq i \leq m$, where $x_{n/3+i}$ belongs to such a pair
  - Case 1: at least $|I|/2$ pairs $(x_{n/3+i}, y_{n/3+i+1})$, $i \in I$, separated in π with respect to the cut
  - Case 2: otherwise

Case 1: many separated pairs $(x_{n/3+i}, y_{n/3+i+1})$

$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3}$ and
$[y]_{n/3}^{n-1} > (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$: $x \cdot y \geq 2^{2n-1}$





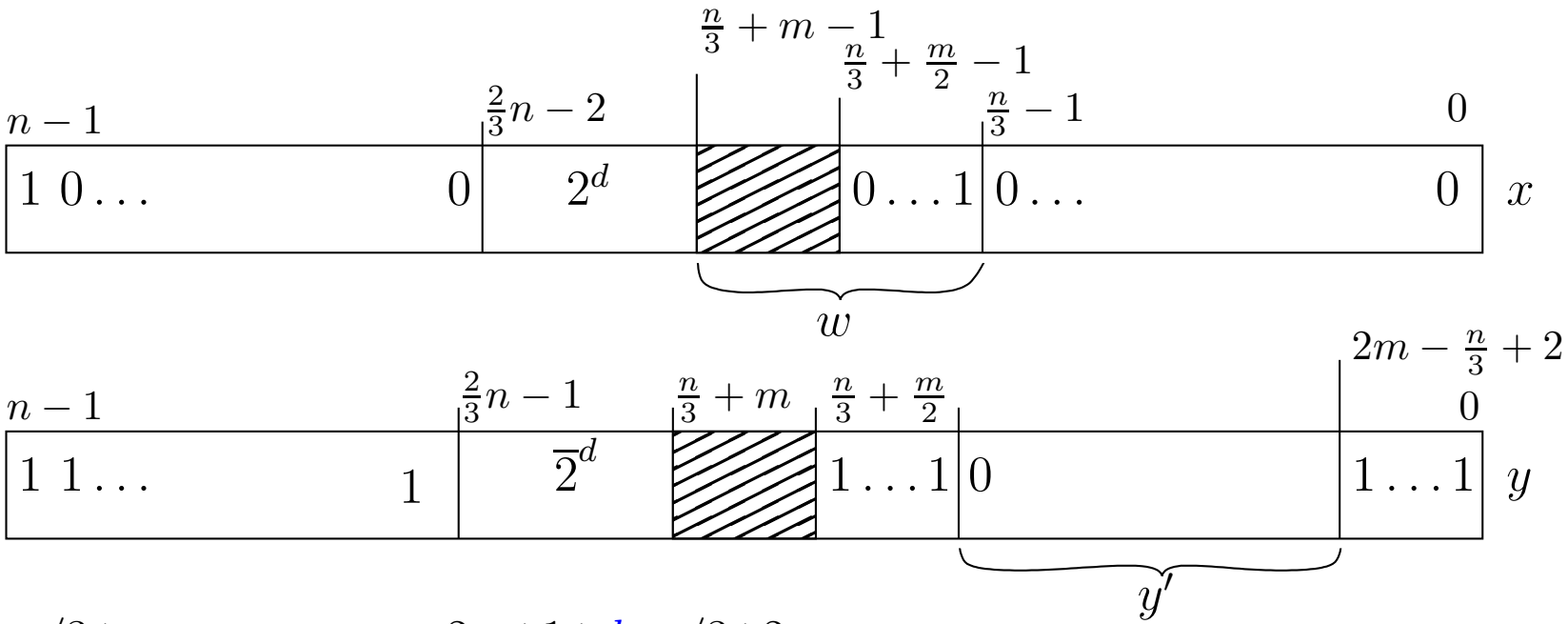
$[x]_{n/3+m/2}^{n/3+m} = w'$: $[y]_{n/3+m/2+1}^{n/3+m+1} \geq 2^{m/2} - 1 - w' \leftrightarrow x \cdot y \geq 2^{2n-1}$

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

Case 2: many pairs $(x_{n/3+i}, y_{n/3+i+1})$ tested together

$[x]_0^{n-1} = 2^{n-1} + \ell\ 2^{n/3}$ and $[y]_{n/3}^{n-1} = (2^n - \ell\ 2^{n/3+1}) \cdot 2^{-n/3}$:

$([y]_0^{n/3-1} \geq \left\lceil \ell^2 2^{-n/3+2} - \frac{4\ell^3}{2^{n-1}+\ell 2^{n/3}} \right\rceil \leftrightarrow x \cdot y \geq 2^{2n-1})$



$[x]_{n/3+m/2}^{n/3+m} = w'$: $[y]_{3m/2+1+d-n/3+2}^{2m+1+d-n/3+2} \geq w' \leftrightarrow x \cdot y \geq 2^{2n-1}$

$[z]_r^l$: integer whose binary representation is $(z_l, \ldots, z_r)$

Concluding remarks

Open: Complexity of $\mathrm{MUL}_{2n-1,n}$ for more general (non-oblivious) BDD-models?

Concluding remarks

Open: Complexity of $\mathrm{MUL}_{2n-1,n}$ for more general (non-oblivious) BDD-models?

Long live the theory of BDDs

Don Knuth, 9th September 2008