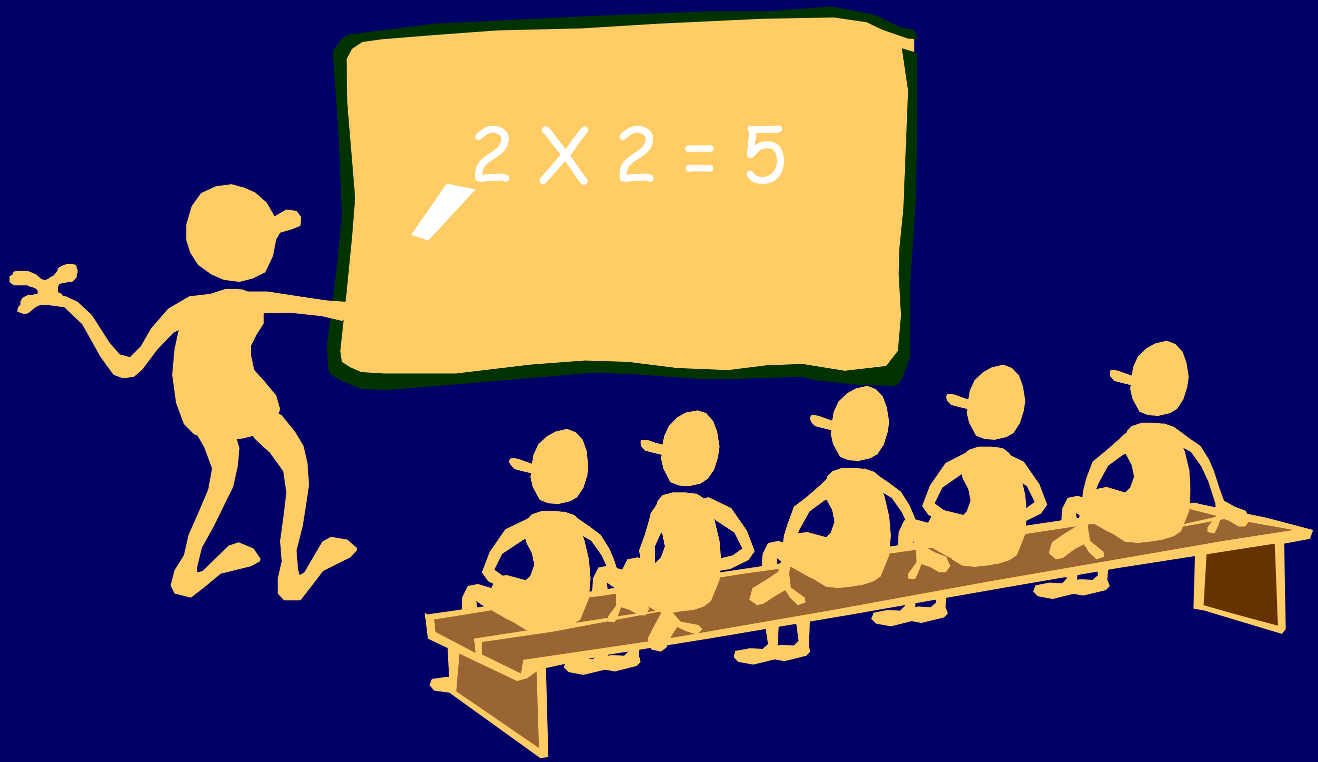
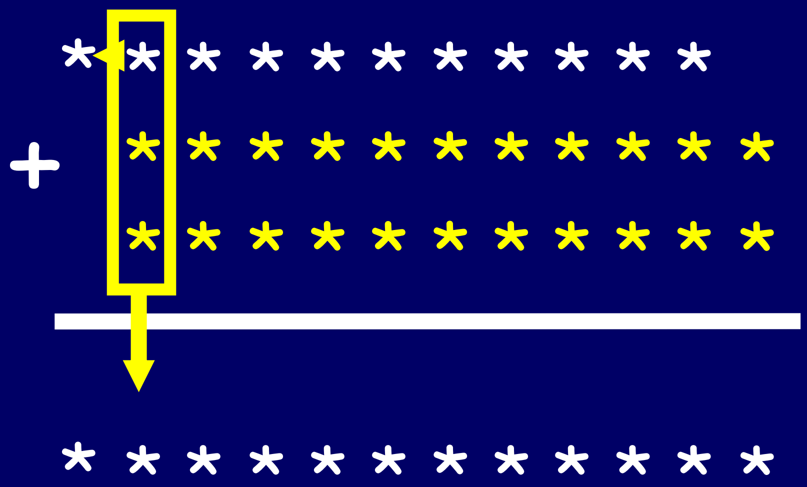
Revisited:
How To Multiply Two Numbers



Time complexity of addition

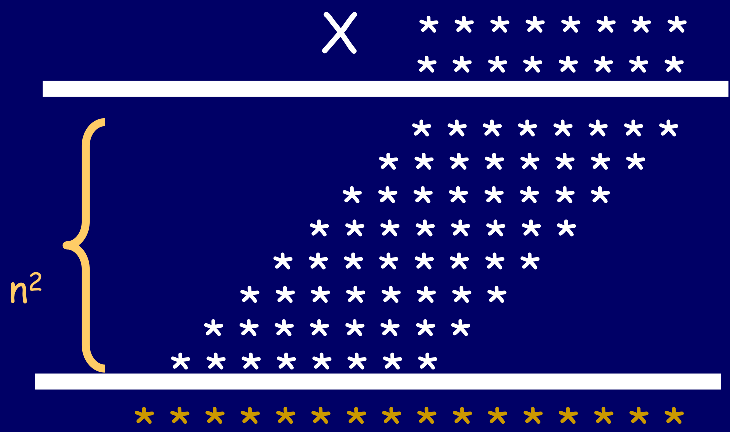


T(n) = The amount of time addition uses to add two n-bit numbers

We saw that T(n) was linear.

$T(n) = \Theta(n)$

Time complexity of school multiplication

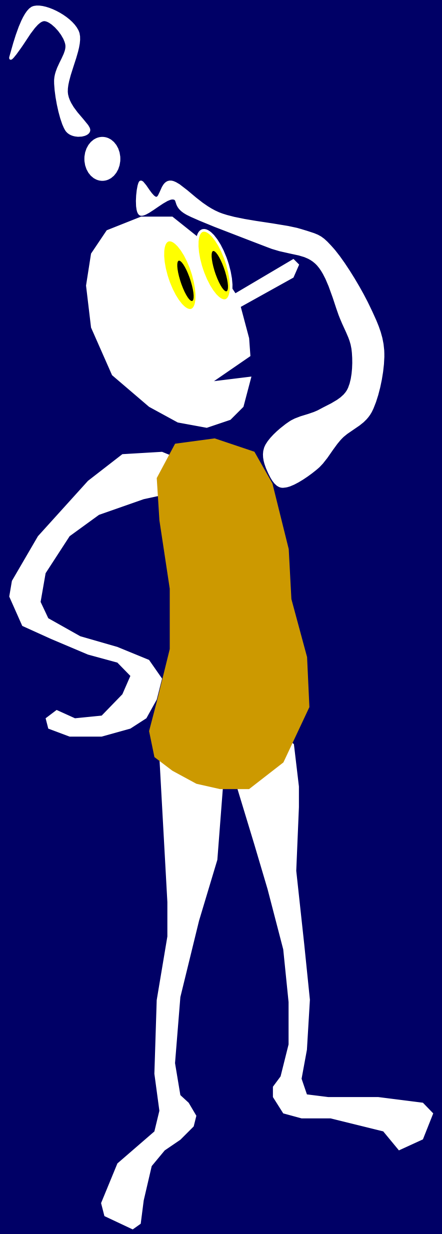


T(n) = The amount of time grade school multiplication uses to add two n-bit numbers

We saw that T(n) was quadratic.

$T(n) = \Theta(n^2)$

addition



Addition is
linear time.

Is there a sub-linear time
method for addition?

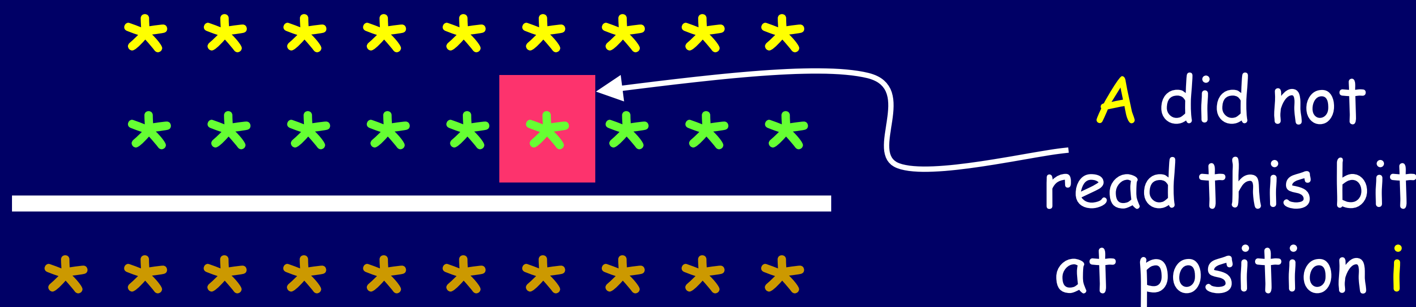
Any addition algorithm takes $\Omega(n)$ time

Claim: Any algorithm for addition must read all of the input bits

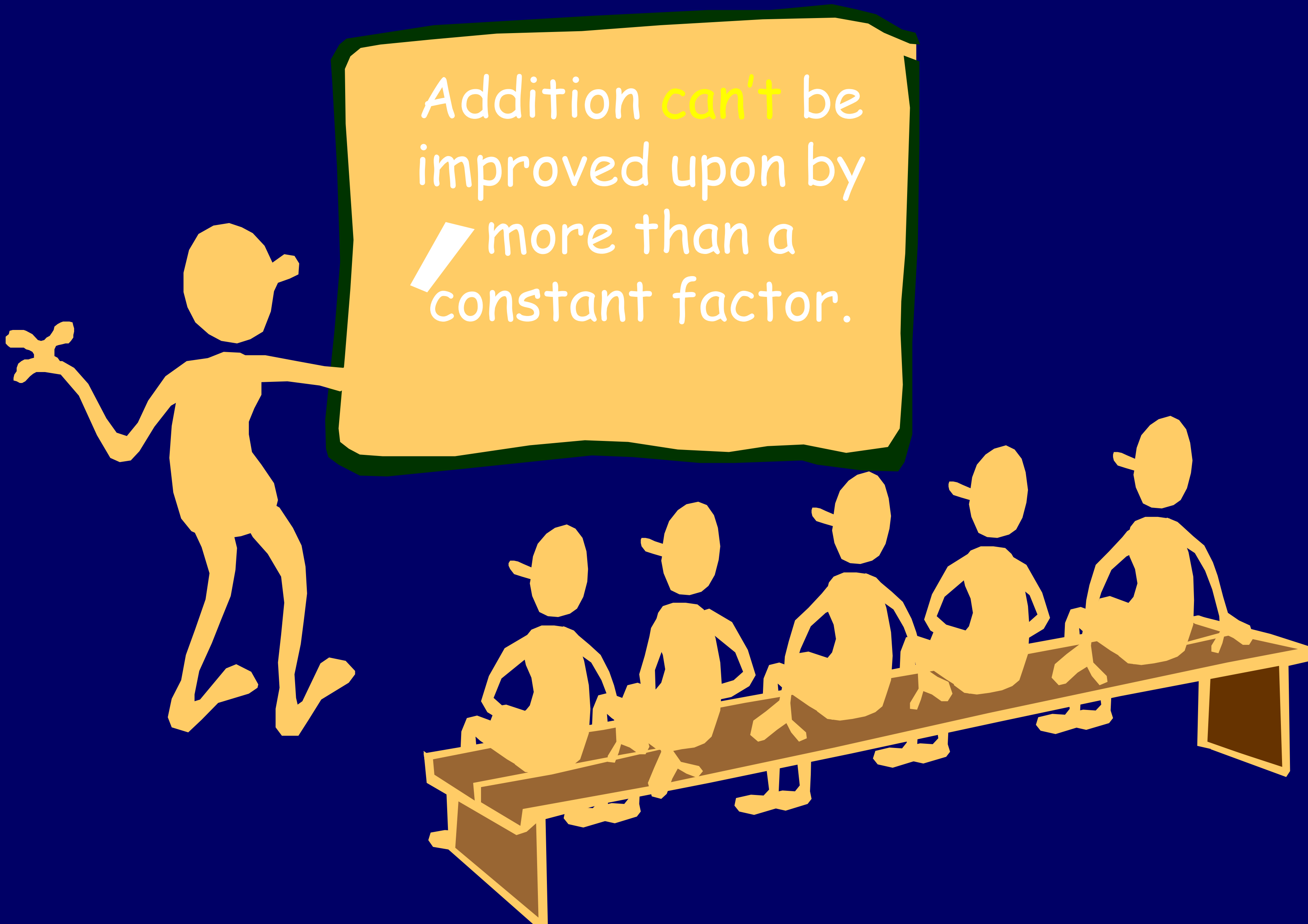
Proof: Suppose there is a mystery algorithm A that does not examine each bit

Give A a pair of numbers. There must be some unexamined bit position i in one of the numbers

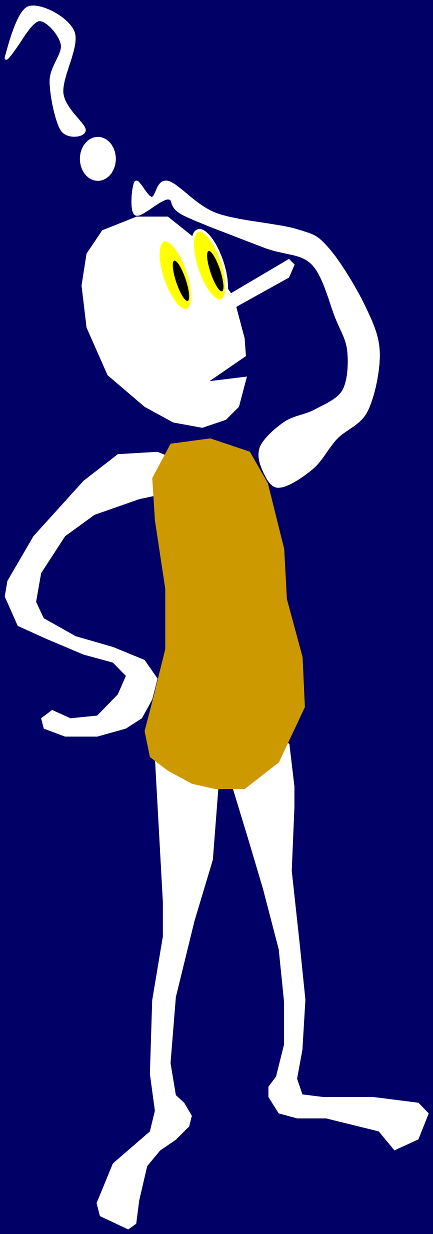
Any addition algorithm takes $\Omega(n)$ time



- If *A* is not correct on the inputs, we found a bug
- If *A* is correct, flip the bit at position *i* and give *A* the new pair of numbers. *A* gives the same answer as before, which is now wrong.

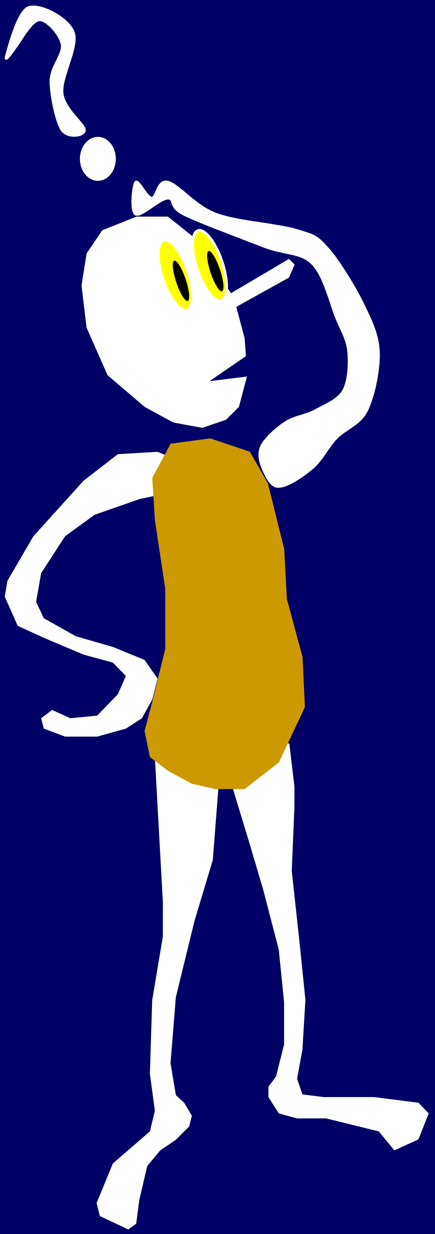

Addition can't be improved upon by more than a constant factor.

Multiplication



Multiplication: $\Theta(n^2)$ time

Is there a clever algorithm to multiply two numbers in <u>linear</u> time?

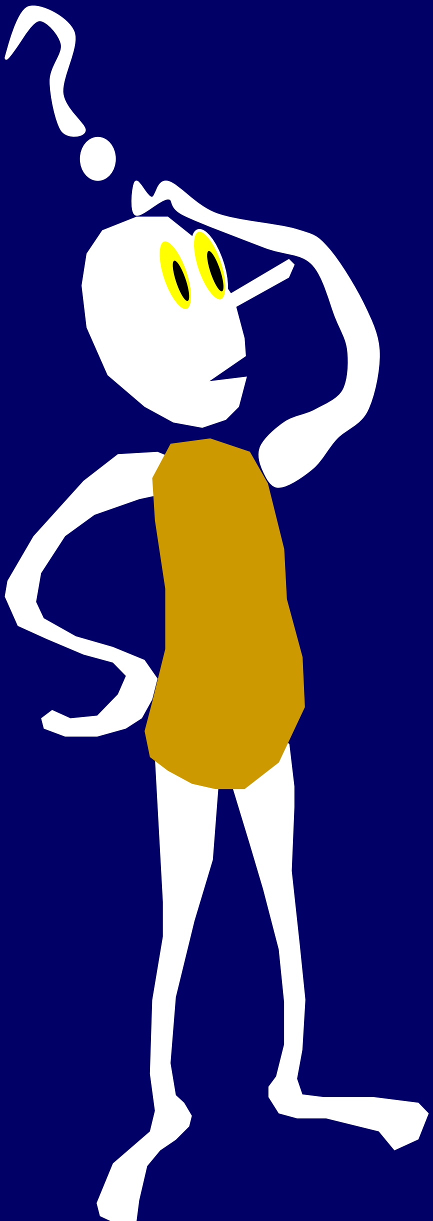


Repetitive addition

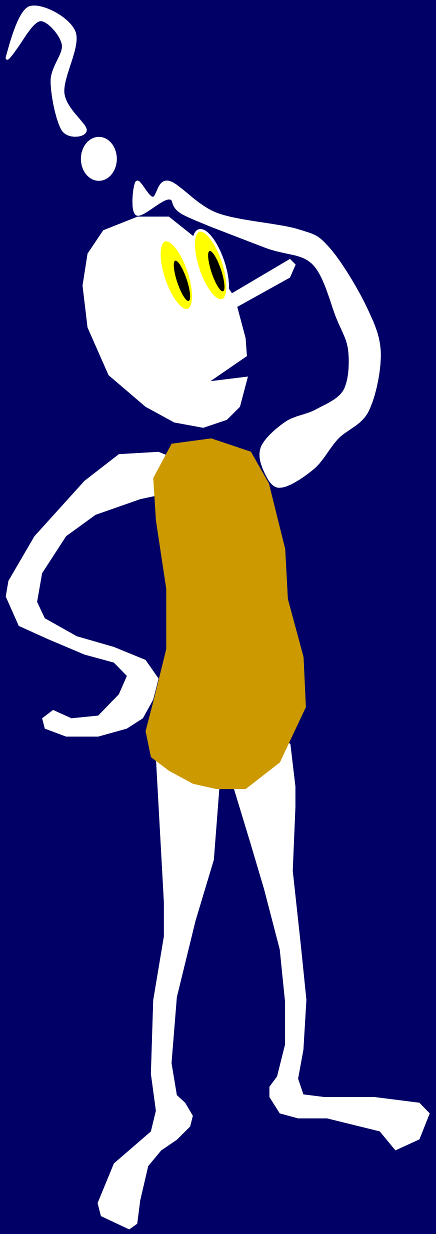
```
int mult( int n, int m)
{
   if( m==0 ) return 0;
   return mult(n, m-1) + n;
}
```

What is the complexity of this algorithm?

Peasant multiplication

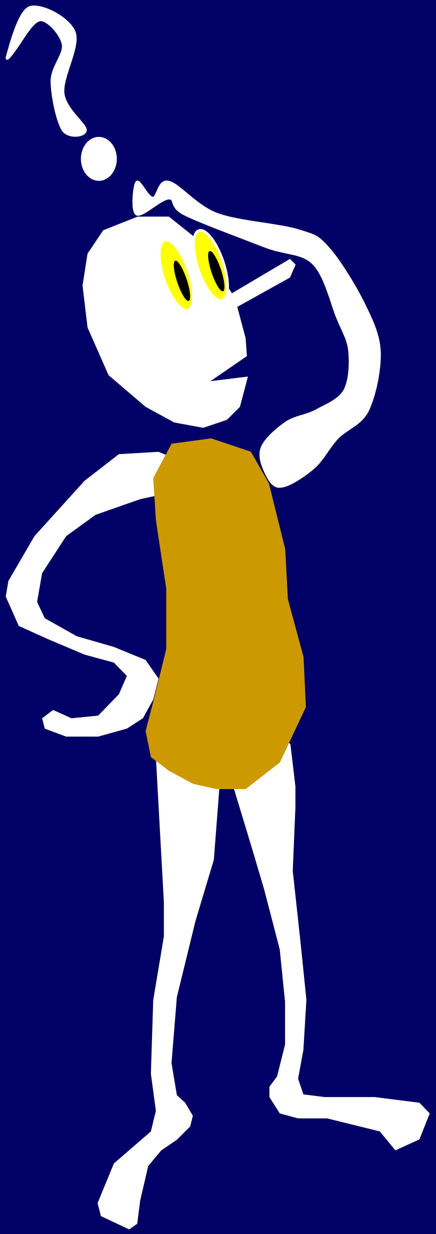


```
   1011
x  1001
 ------
   1011
  0000
 0000
1011
----------
1100011
```



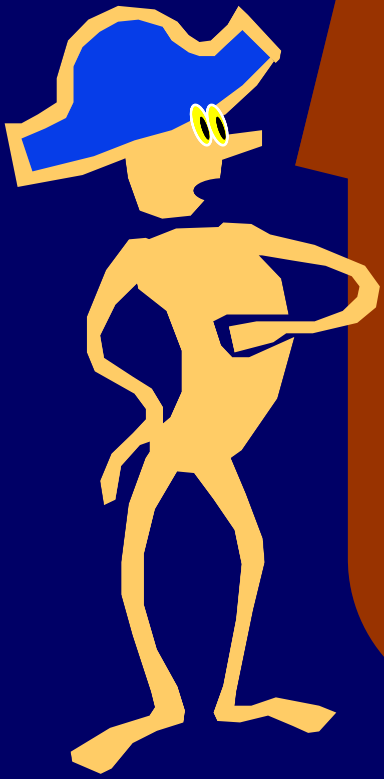
Peasant multiplication

Why is it called the "Russian" peasant's algorithm?



Peasant multiplication

It's also called the Egyptian multiplication.



But if the number does not fit the CPU?

Can we do something very different than grade school multiplication?

Divide And Conquer

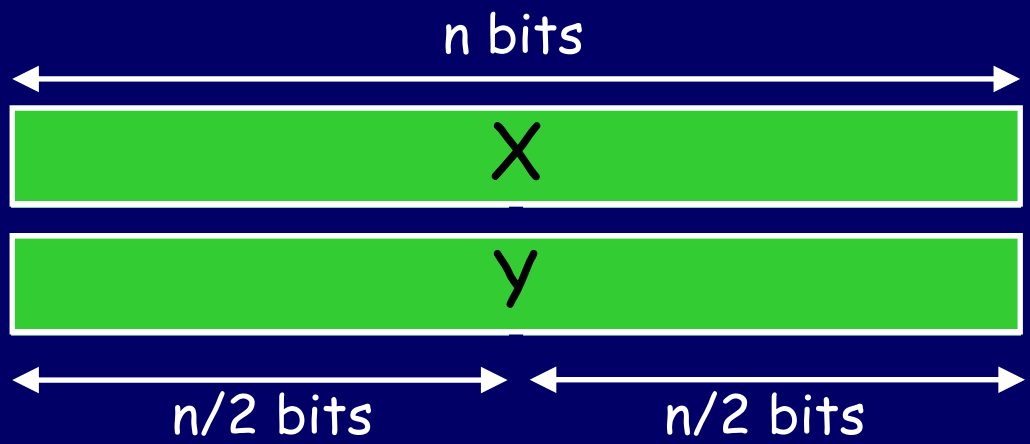
An approach to faster algorithms:

1. DIVIDE a problem into smaller subproblems

2. CONQUER them recursively

3. GLUE the answers together so as to obtain the answer to the larger problem

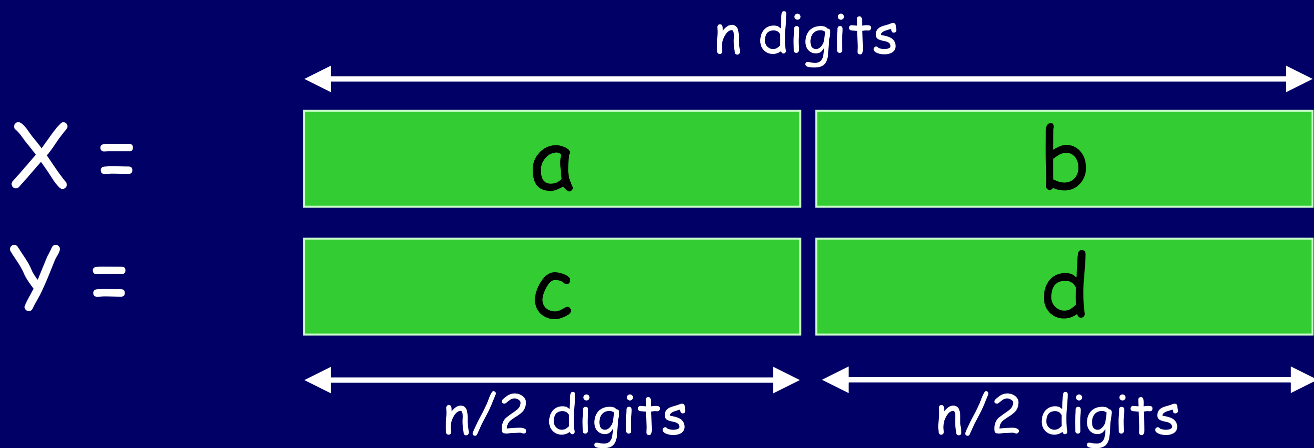
Multiplication of 2 n-bit numbers

$X =$ 
$Y =$

$$X = a\,2^{n/2} + b \qquad Y = c\,2^{n/2} + d$$

$$X \times Y = ac\,2^{n} + (ad + bc)\,2^{n/2} + bd$$

Same thing for decimals



$$X = a\,10^{n/2} + b \qquad Y = c\,10^{n/2} + d$$

$$X \times Y = ac\,10^{n} + (ad + bc)\,10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139

X = | a | b |
Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^{n} + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

X =	a	b
Y =	c	d

$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21 12*39

X = a b

Y = c d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21 12*39 34*21

X = a b

Y = c d

$$X \times Y = ac\ 10^{n} + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

12*21   12*39   34*21   34*39

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21 12*39 34*21 34*39

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^{n} + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21 12*39 34*21 34*39

1*2 1*1 2*2 2*1

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

12*21 12*39 34*21 34*39

2 1 4 2

Hence: $12*21 = 2*10^2 + (1 + 4)10^1 + 2 = 252$

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

252   12*39   34*21   34*39

2   1   4   2

Hence: $12*21 = 2*10^2 + (1 + 4)10^1 + 2 = 252$

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

252 12*39 34*21 34*39

Hence: $12*21 = 2*10^2 + (1 + 4)10^1 + 2 = 252$

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

252 12*39 34*21 34*39

1*3 1*9 2*3 2*9

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^{n} + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

242 12*39 34*21 34*39

3 9 6 18

$*10^2 + *10^1 + *10^1 + *1$

X = | a | b |

Y = | c | d |

$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

242   468   34*21   34*39

3   9   6   18

$*10^2 + *10^1 + *10^1 + *1$

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

252   468   714   1326

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^{n} + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139   1234*4276   5678*2139   5678*4276

252 $*10^4$ + 468 $*10^2$ + 714 $*10^2$ + 1326 $*1$

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

1234*2139 1234*4276 5678*2139 5678*4276

252 468 714 1326

$*10^4 + *10^2 + *10^2 + *1$

= 2639526

X = a b

Y = c d

$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$

Multiplying (Divide & Conquer style)

12345678 * 21394276

2639526 1234*4276 5678*2139 5678*4276

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

2639526 5276584 12145242 24279128

X =	a	b
Y =	c	d

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

2639526	5276584	12145242	24279128
$*10^8$ +	$*10^4$ +	$*10^4$ +	$*1$

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

Multiplying (Divide & Conquer style)

12345678 * 21394276

2639526 $*10^8$	+	5276584 $*10^4$	+	12145242 $*10^4$	+	24279128 $*1$

= 264126842539128

X = | a | b |

Y = | c | d |

$$X \times Y = ac\ 10^n + (ad + bc)\ 10^{n/2} + bd$$

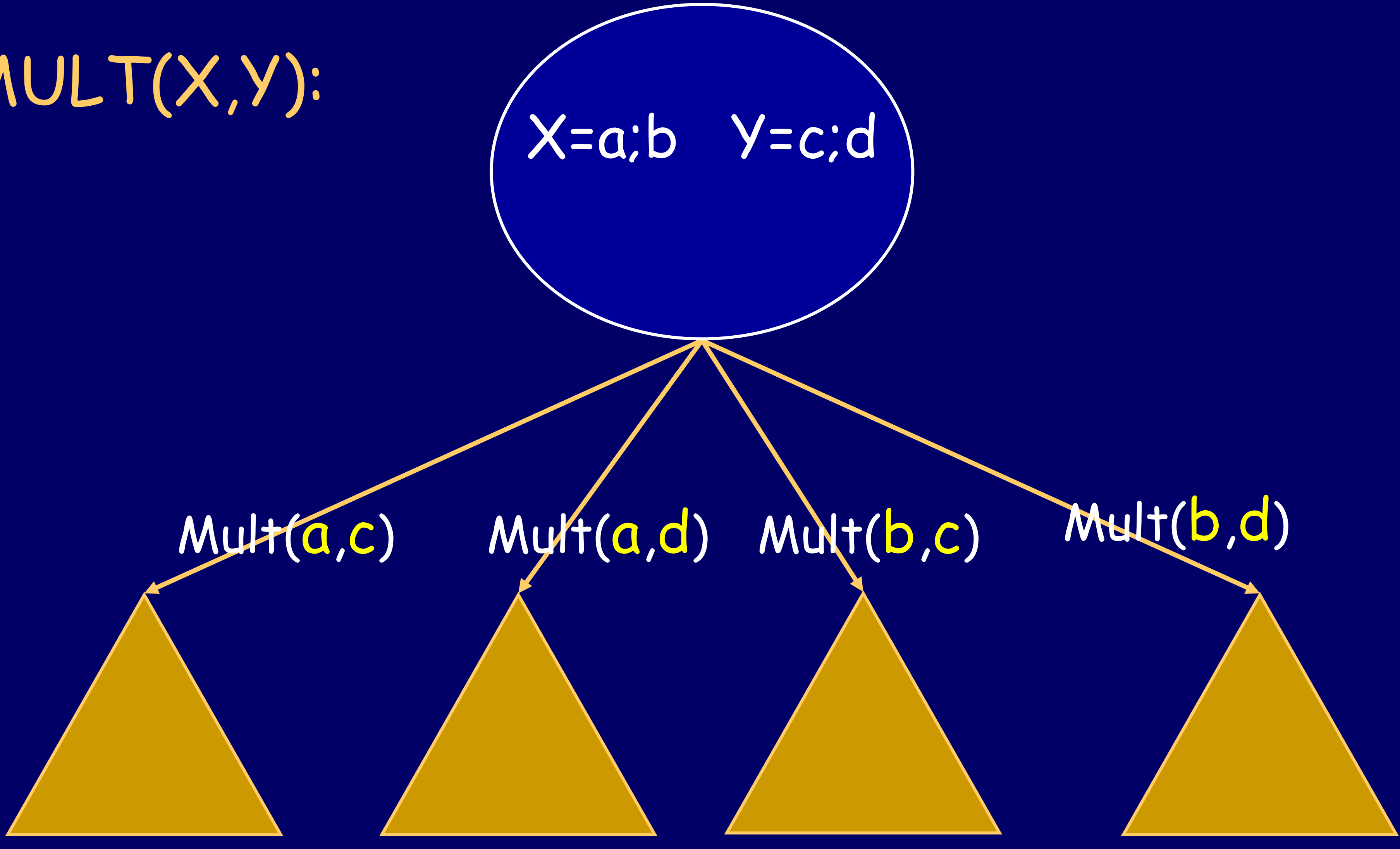
Divide, Conquer, and Glue

MULT(X,Y):

X=a;b Y=c;d

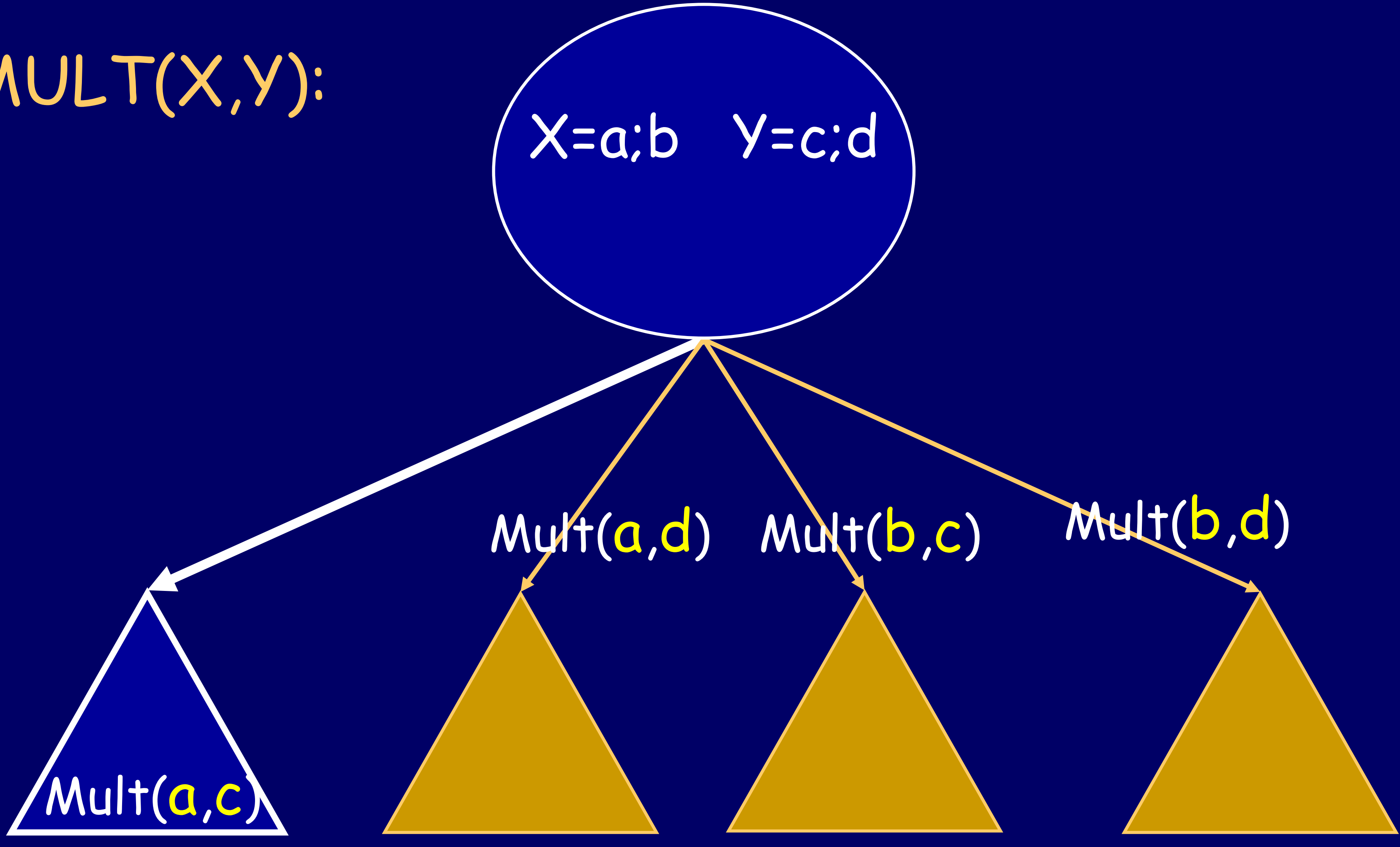
Divide, Conquer, and Glue

MULT(X,Y):



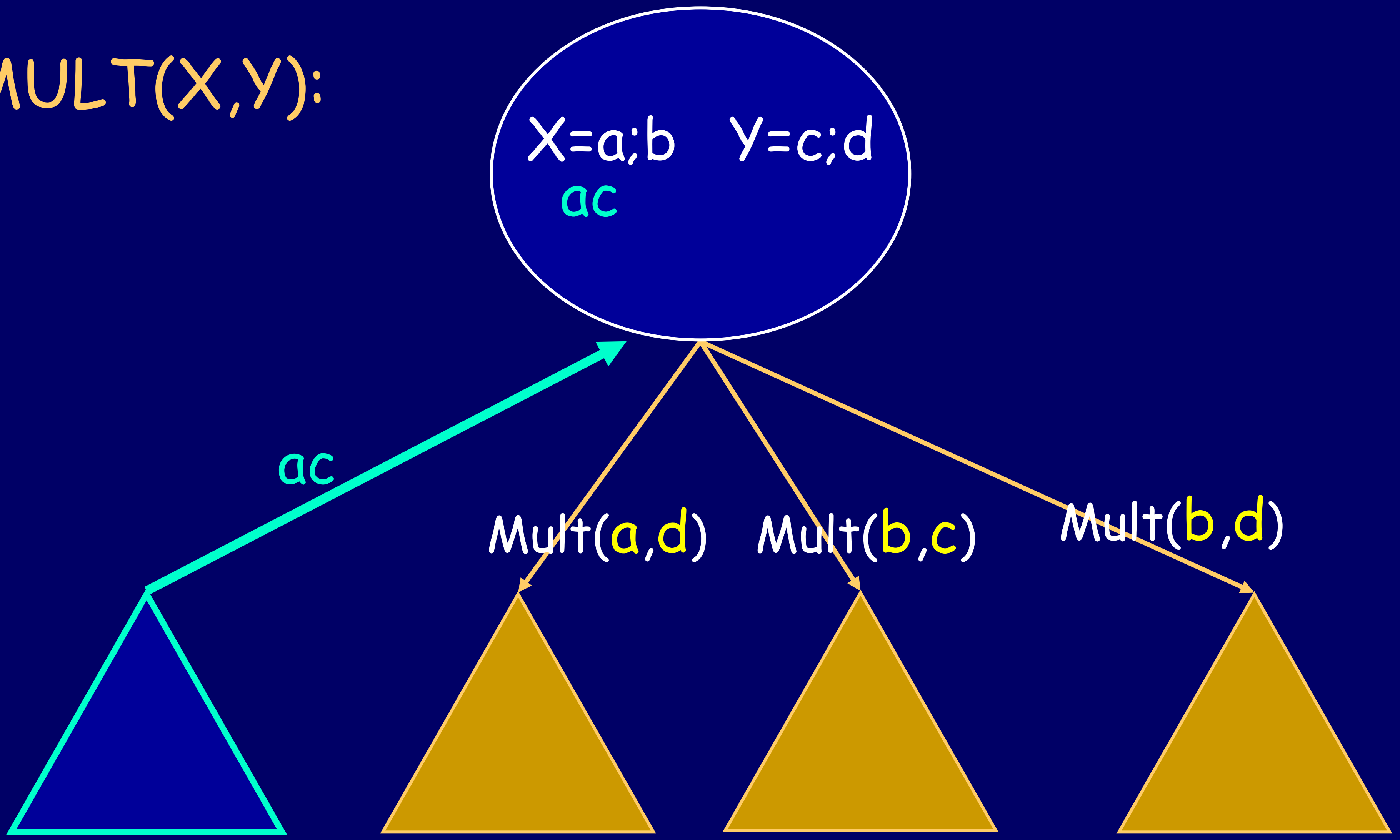
Divide, Conquer, and Glue

MULT(X,Y):



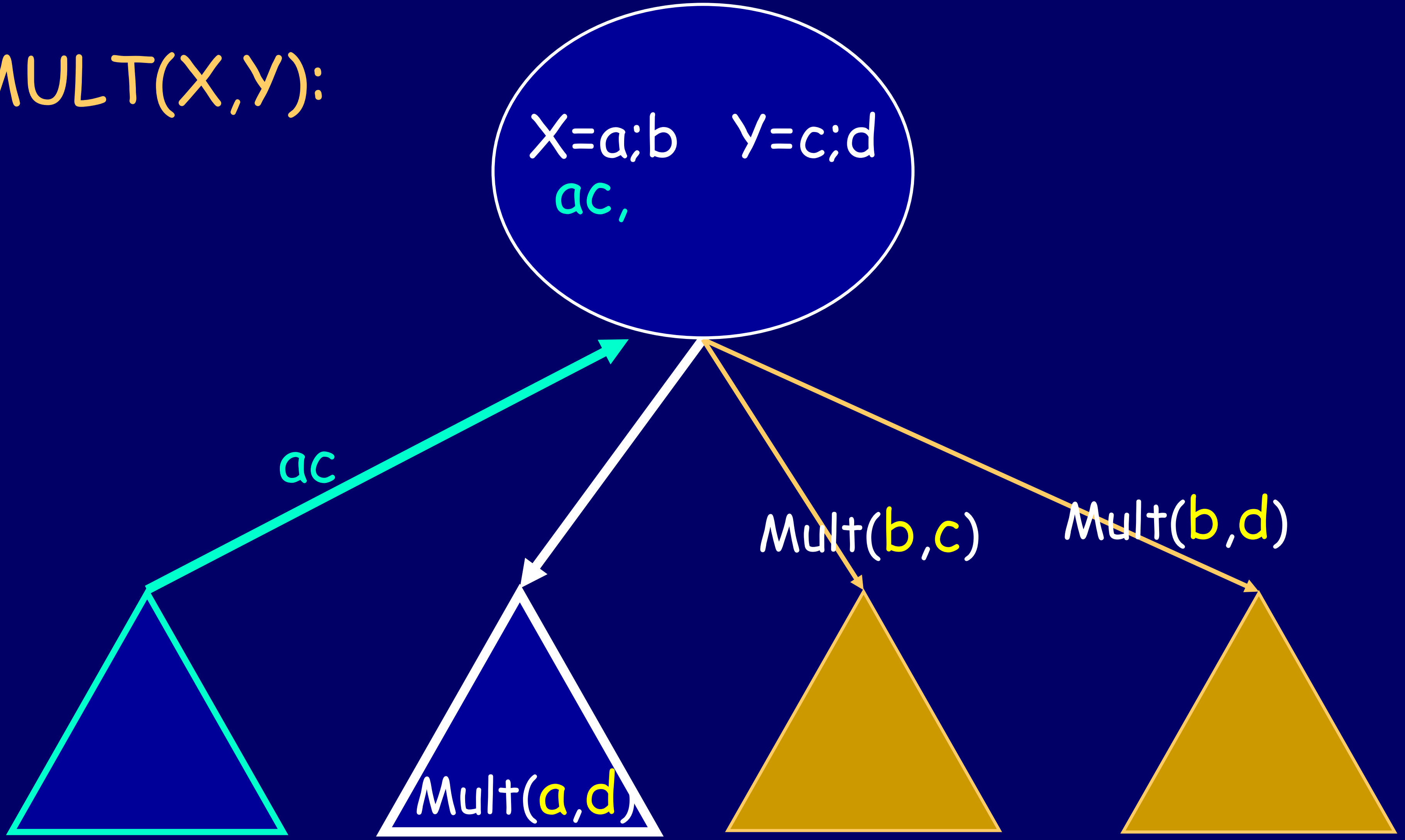
Divide, Conquer, and Glue

MULT(X,Y):



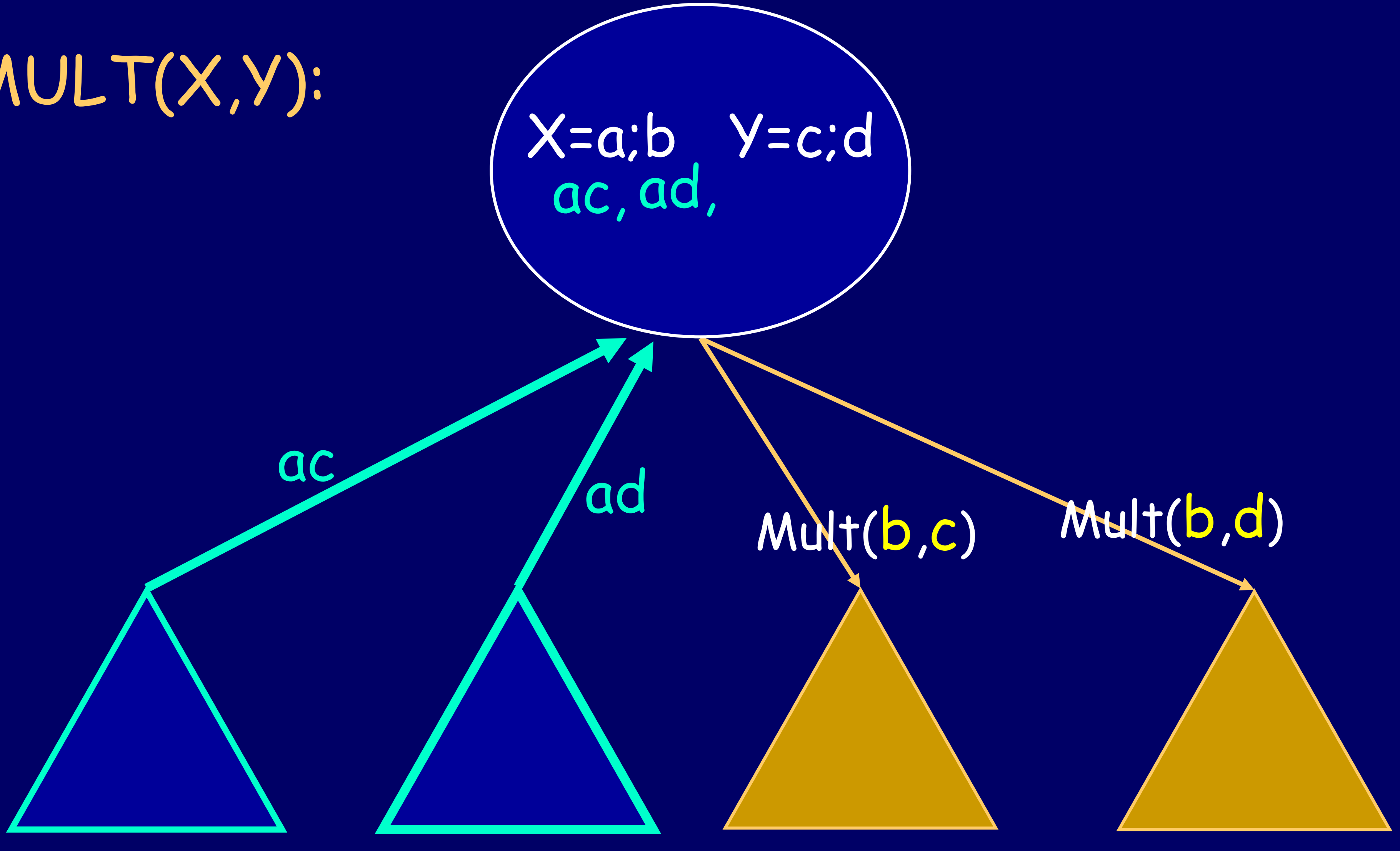
Divide, Conquer, and Glue

MULT(X,Y):



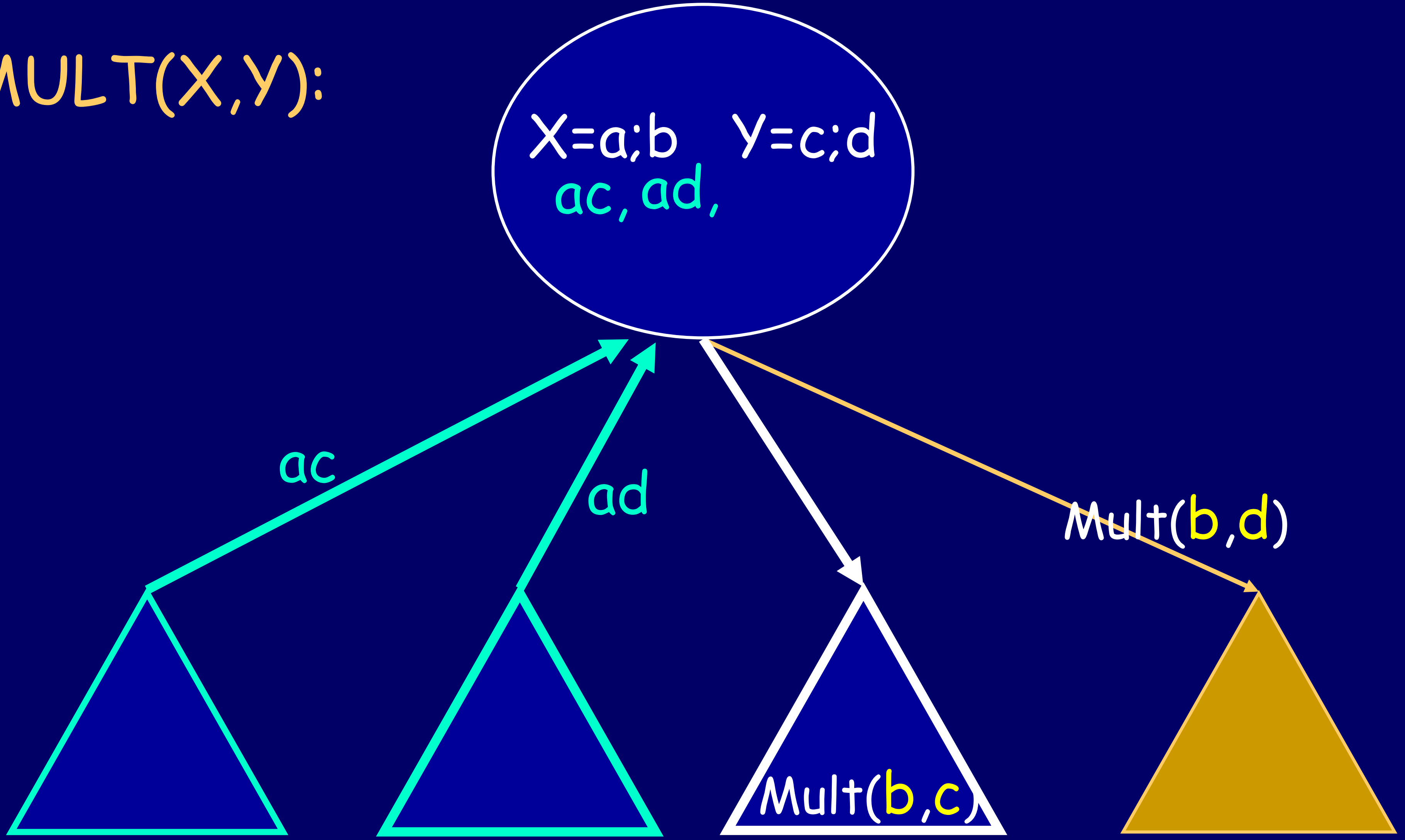
Divide, Conquer, and Glue

MULT(X,Y):



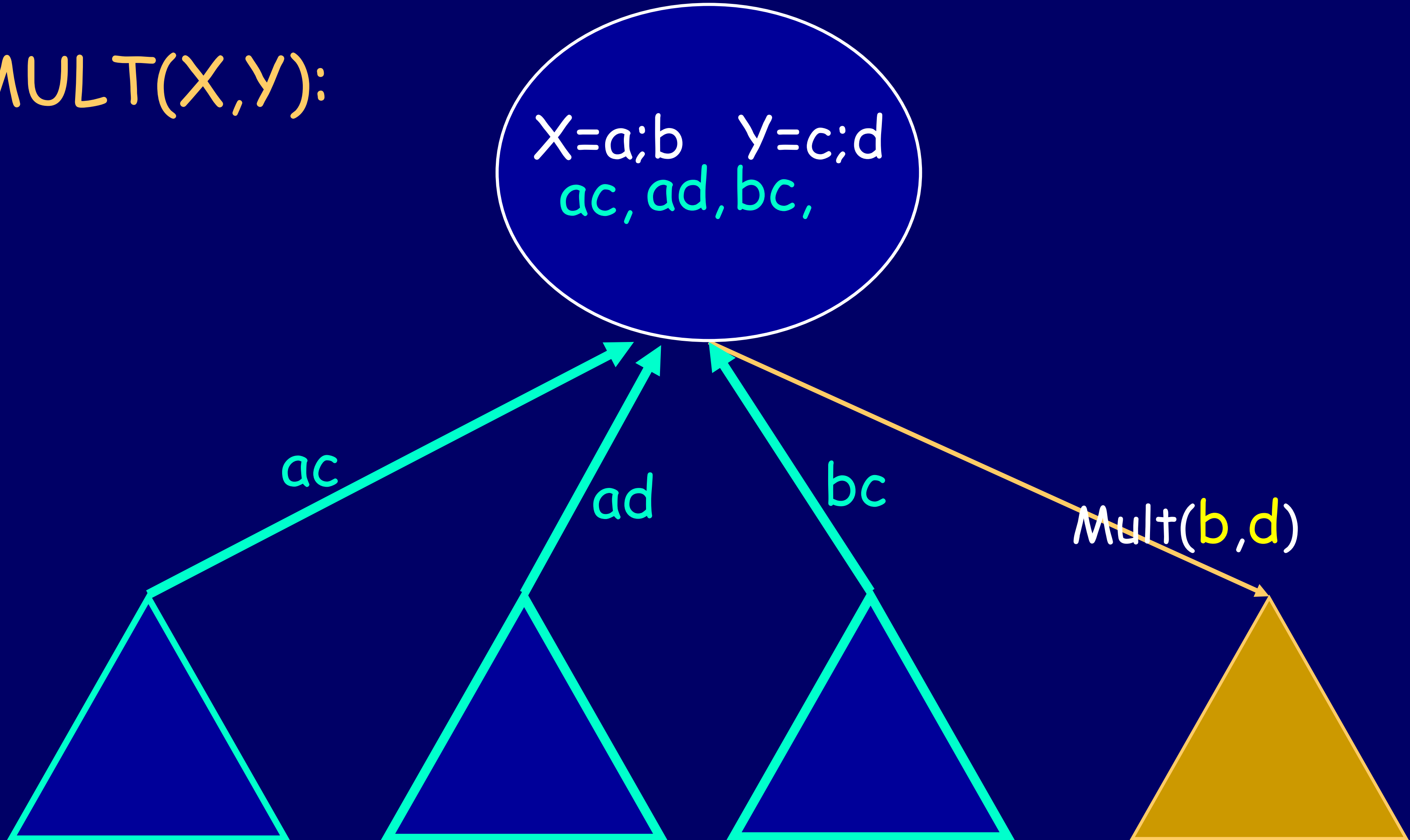
Divide, Conquer, and Glue

MULT(X,Y):



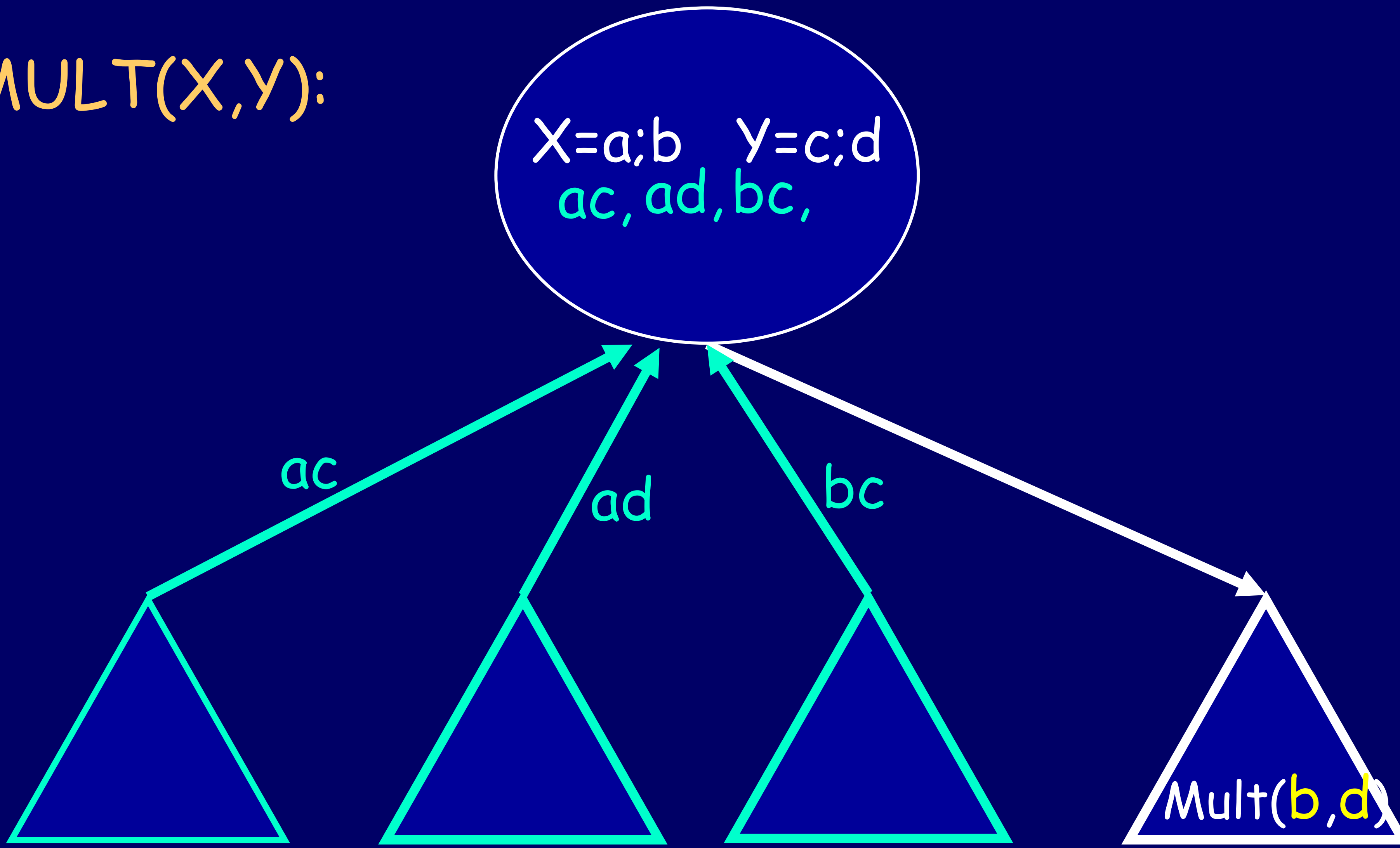
Divide, Conquer, and Glue

MULT(X,Y):



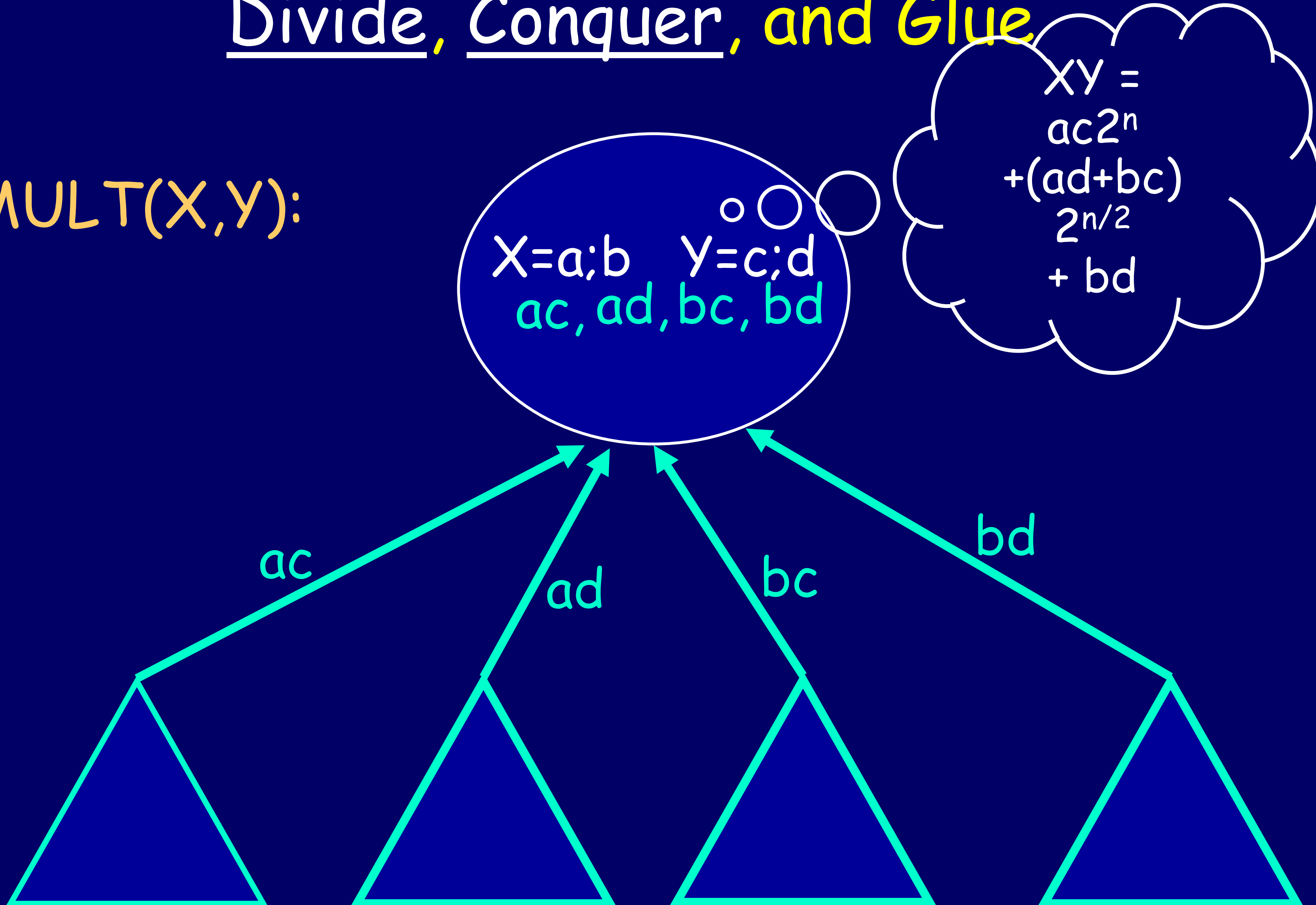
Divide, Conquer, and Glue

MULT(X,Y):



Divide, Conquer, and Glue

MULT(X,Y):



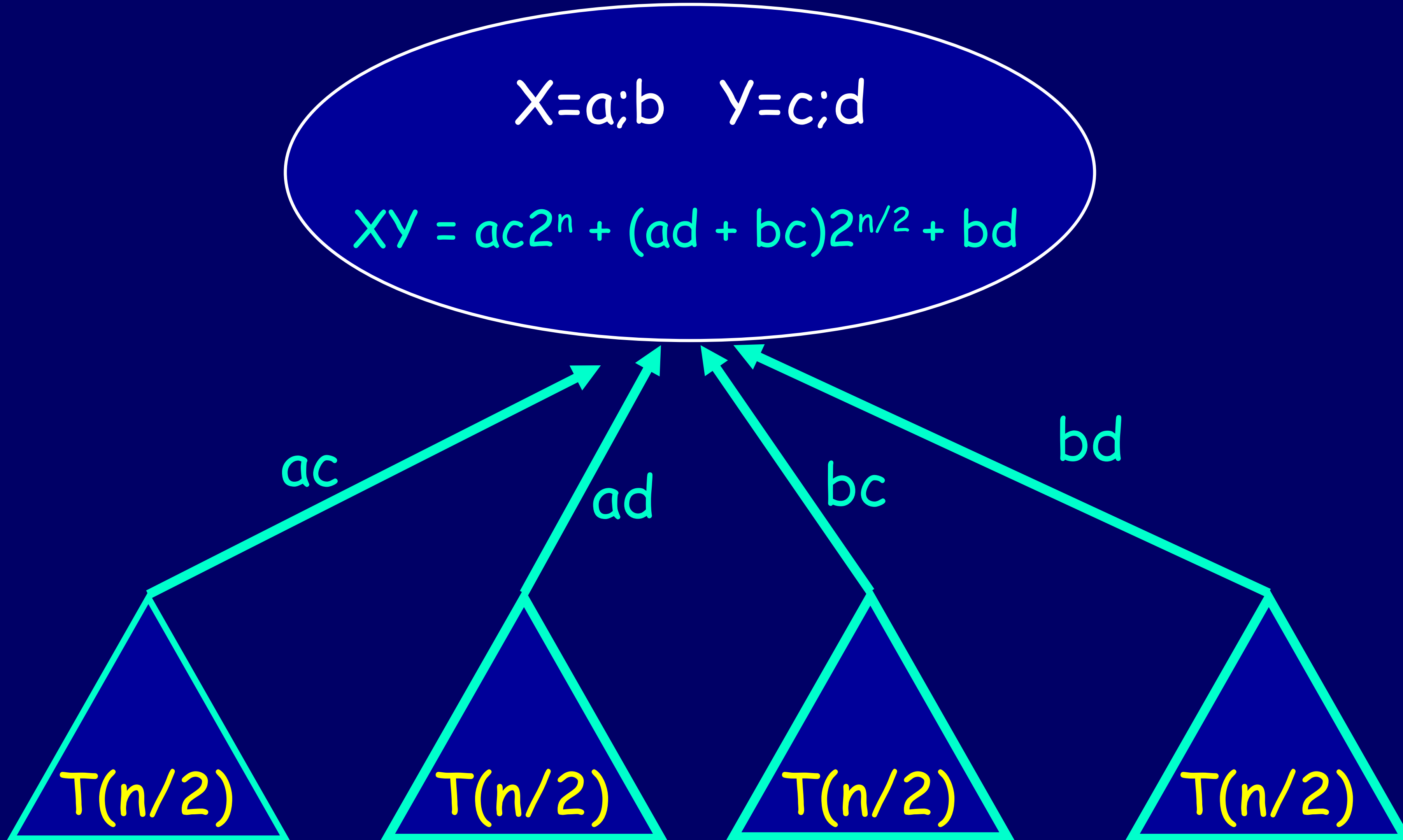
Time required by MULT

$T(n)$ = time taken by MULT on two n-bit numbers

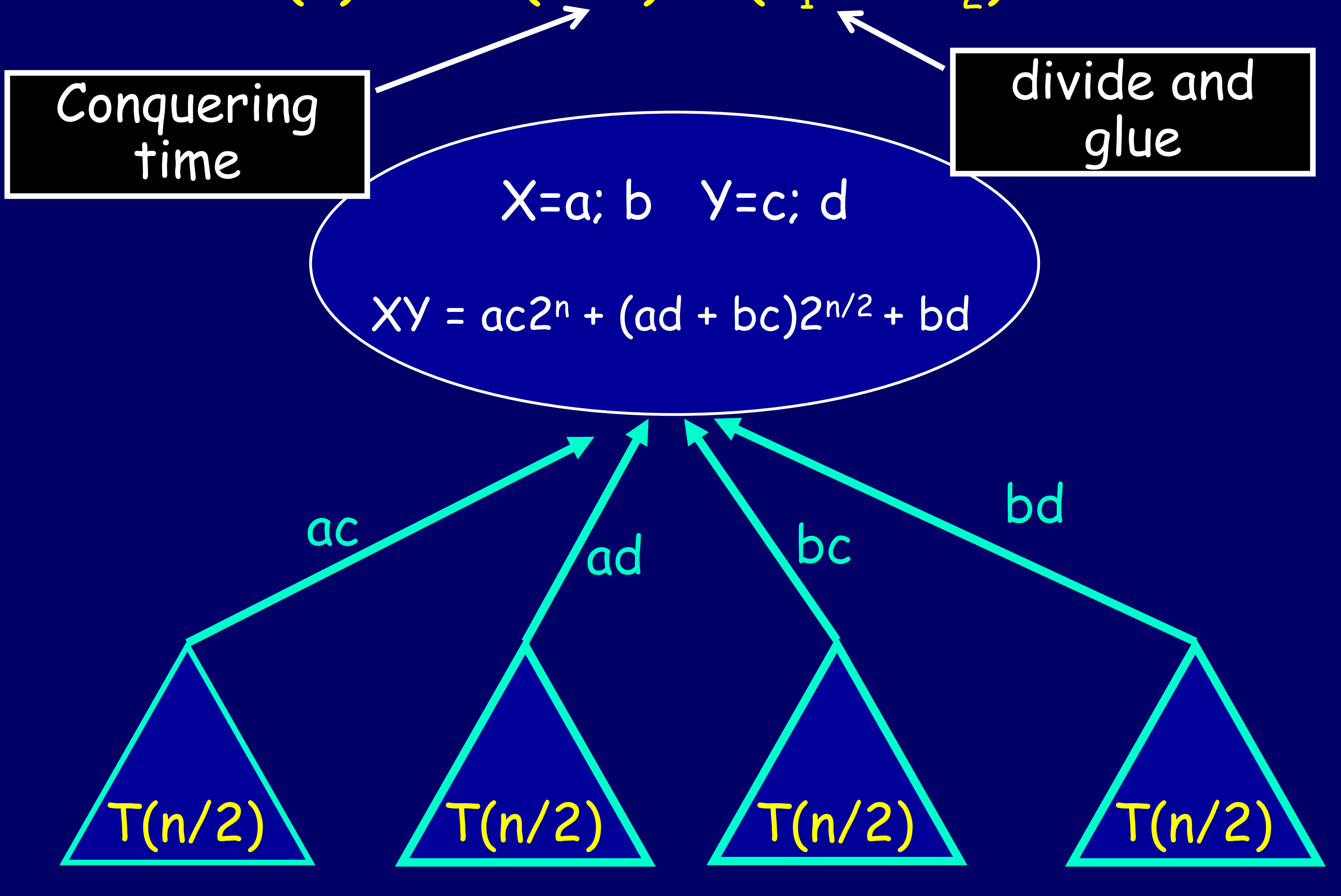
What is $T(n)$? What is its growth rate?

Big Question: Is it $\Theta(n^2)$?

Time required by MULT



$$T(n) = 4\,T(n/2) + (c_1 n + c_2)$$



Recurrence Relation

$T(1) = c_3$

$T(n) = 4\ T(n/2) + c_1\ n + c_2$

What is the growth rate of T(n)?

Let's keep it simple

$T(1) = 1$

$T(n) = 4\,T(n/2) + n$

What is the growth rate of $T(n)$?

Technique: Guess and Verify

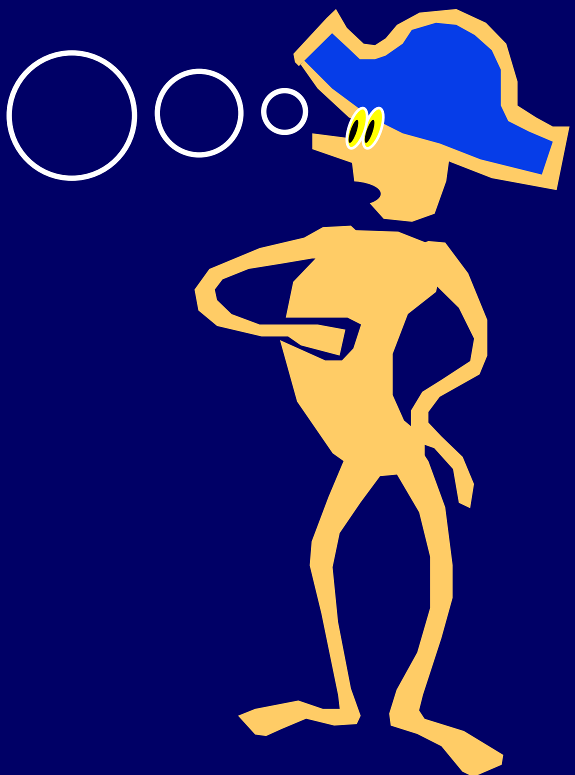
Guess: $T(n) = 2n^2 - n$

Verify: $T(1) = 1$ and $T(n) = 4\,T(n/2) + n$

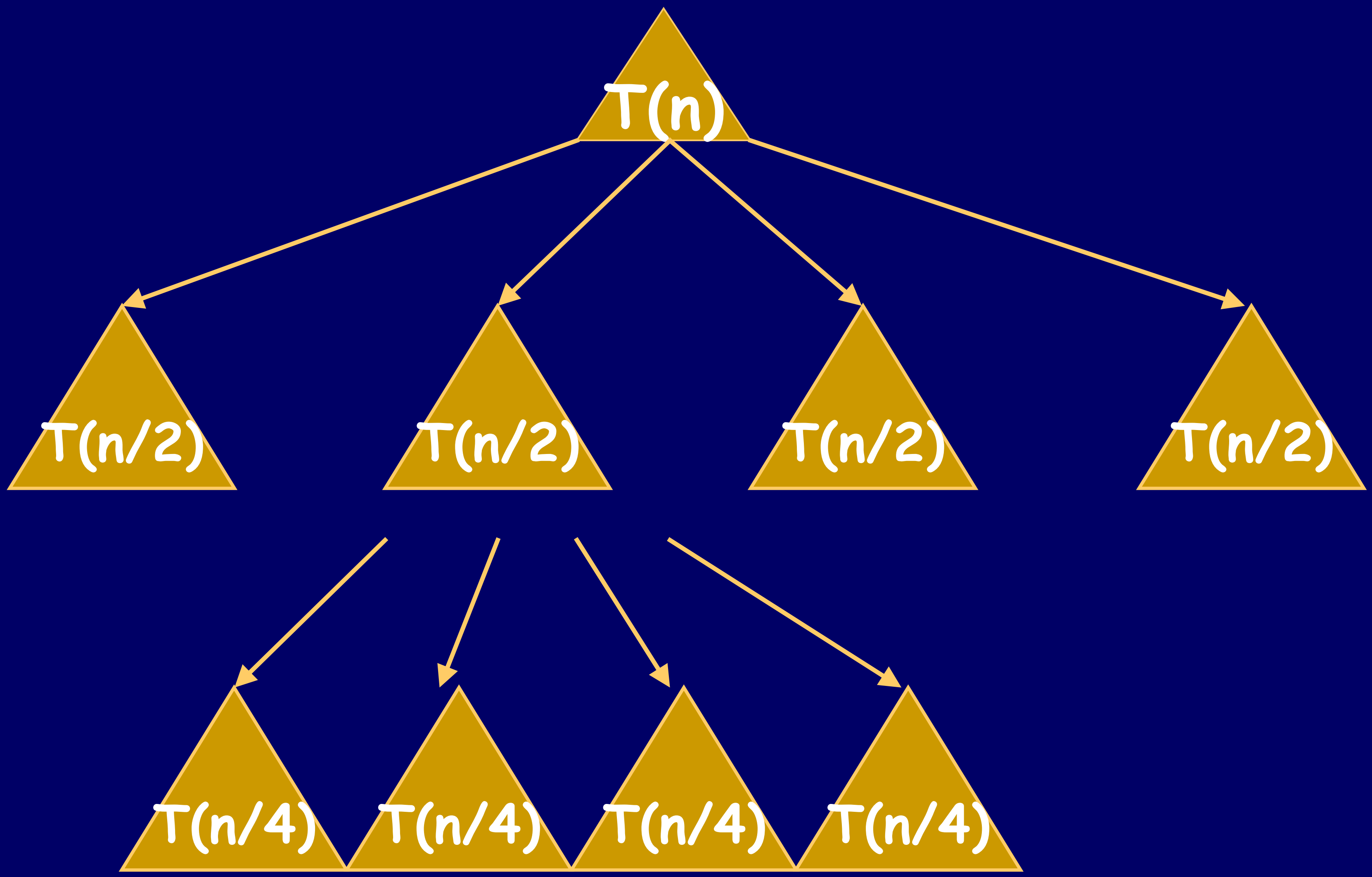
$$
\begin{aligned}
2n^2 - n &= 4\,[2(n/2)^2 - n/2] + n \\
&= 2n^2 - 2n + n \\
&= 2n^2 - n
\end{aligned}
$$

Recursion Tree Representation

We visualize the recursion as a tree, where each node represents a recursive call. The root is the initial call. Leaves correspond to the exit condition.

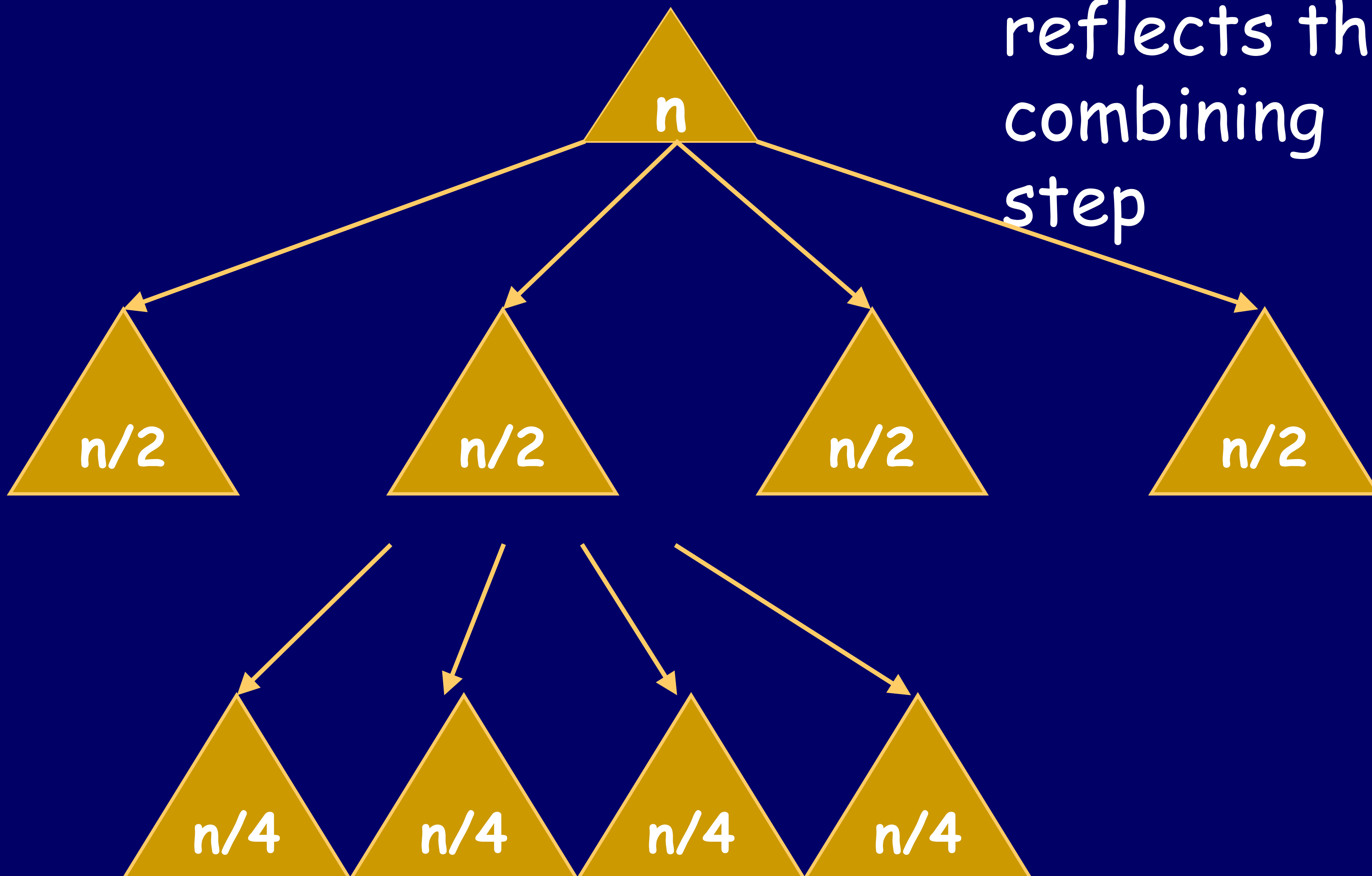


$$T(n) = 4\,T(n/2) + n$$



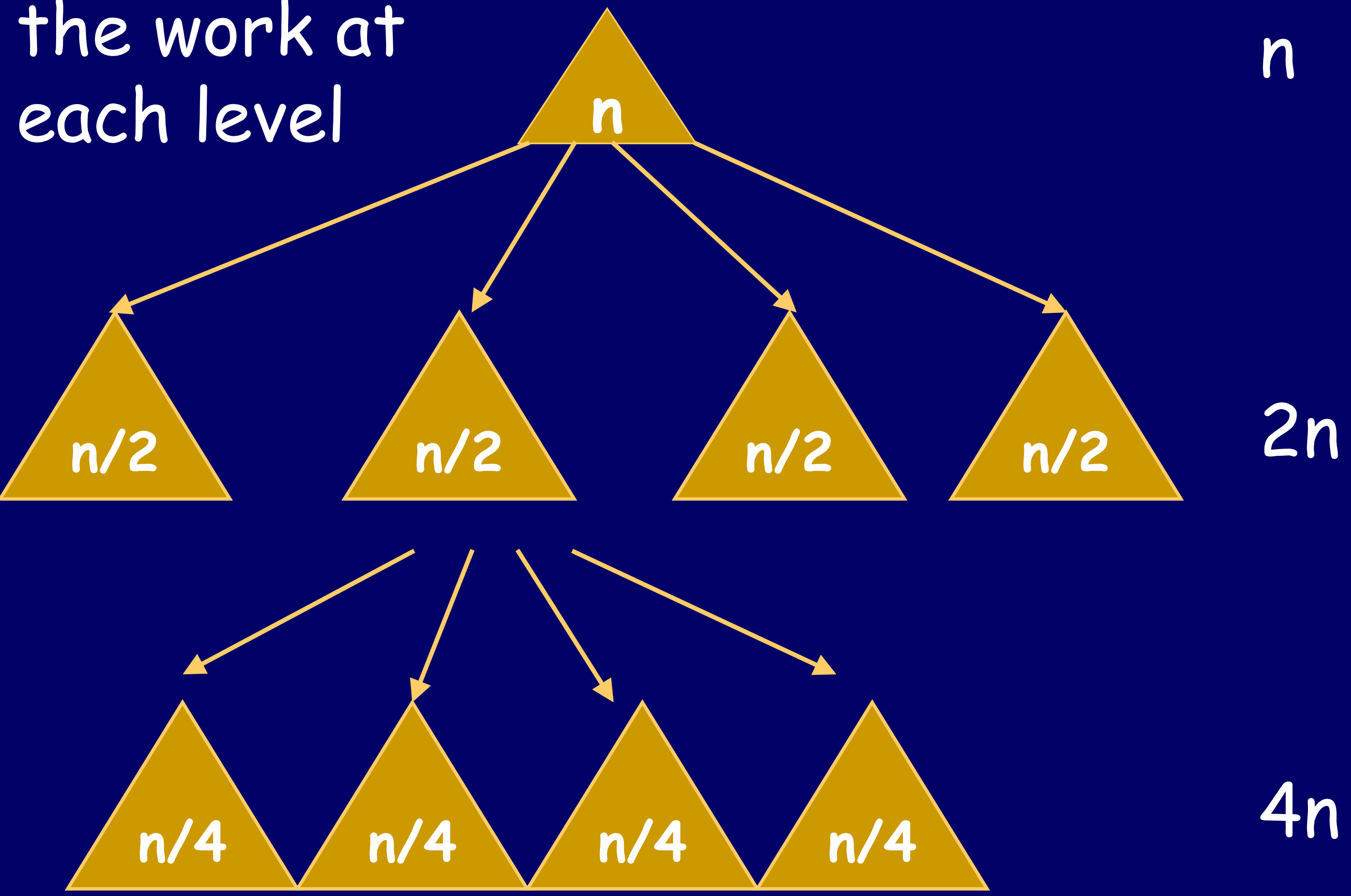
Recursion Tree

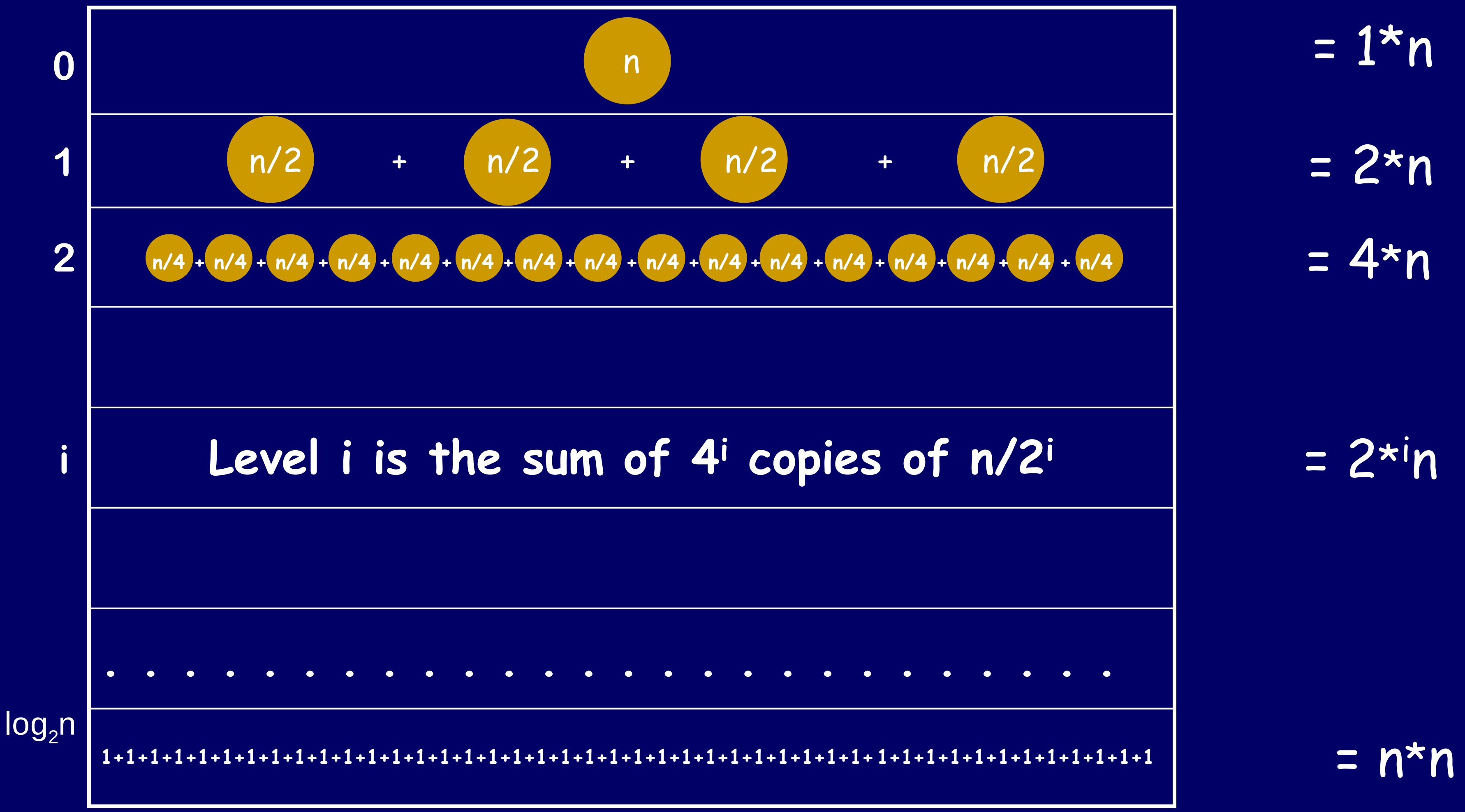
each node reflects the combining step



Recursion Tree

write down the work at each level

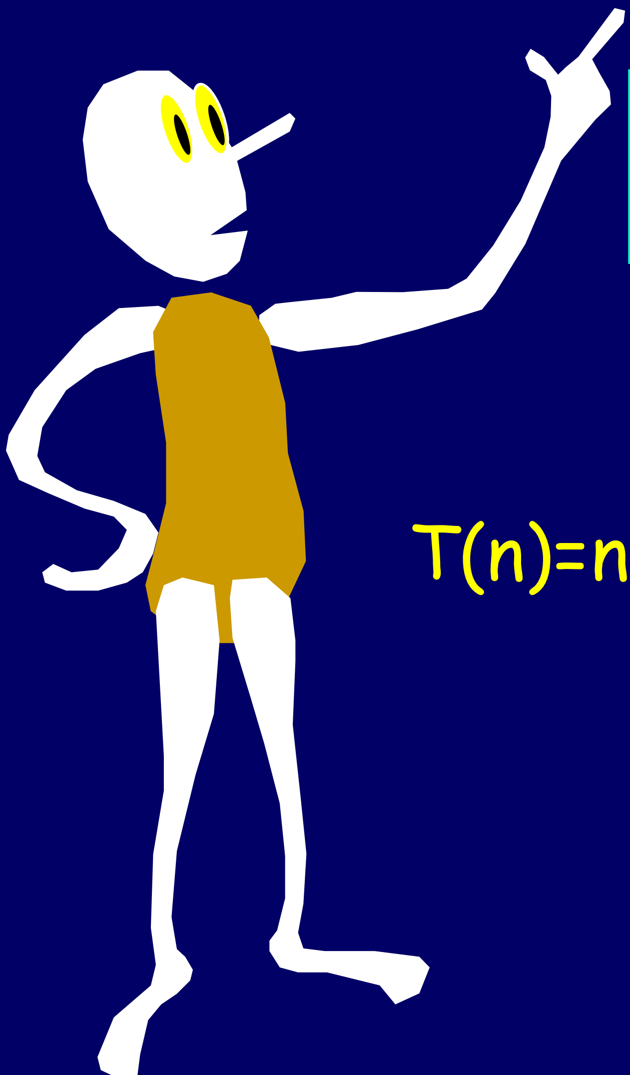




$$T(n)=n\,(1+2+4+8+\ .\ .\ .\ +2^h),\ \text{where } h = \log_2 n$$

$$T(n) = n(2n-1) = \Theta(n^2)$$

$$1 + X^1 + X^2 + X^3 + \ldots + X^{n-1} + X^n = \frac{X^{n+1} - 1}{X - 1}$$



The Geometric Series

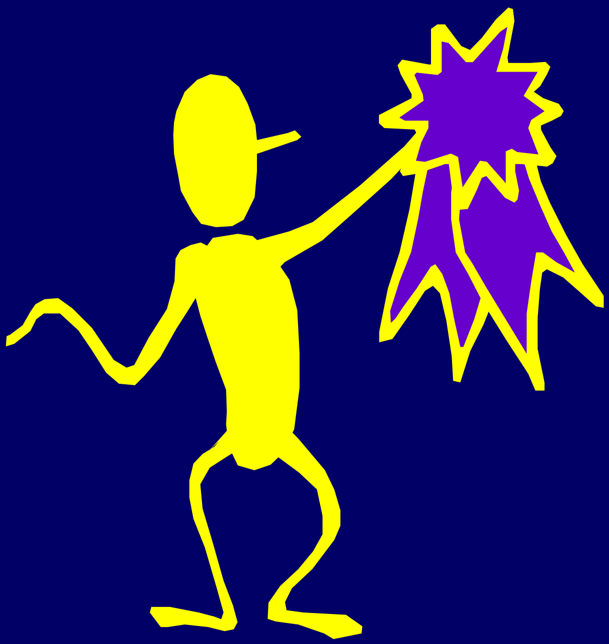
$T(n) = n\,(1+2+4+8+\ .\ .\ .\ +2^h)$, where $h = \log_2 n$

$T(n) = n(2n-1) = \Theta(n^2)$

Divide and Conquer MULT: $\Theta(n^2)$ time

Multiplication: $\Theta(n^2)$ time

Karatsuba, Anatolii Alexeevich (1937-)



In 1962 Karatsuba had formulated the first algorithm to break n^2 barrier!

Multiplication of 2 n-bit numbers

$X = a\,2^{n/2} + b \qquad Y = c\,2^{n/2} + d$

$X \times Y = ac\,2^{n} + (ad + bc)\,2^{n/2} + bd$

$z1 = (a + b)(c + d) = ac + ad + bc + bd$

$z2 = ac$

$z3 = bd$

$z4 = z2 - z3 \qquad = ac - bd$

$z5 = z1 - z2 - z3 = ad + bc$

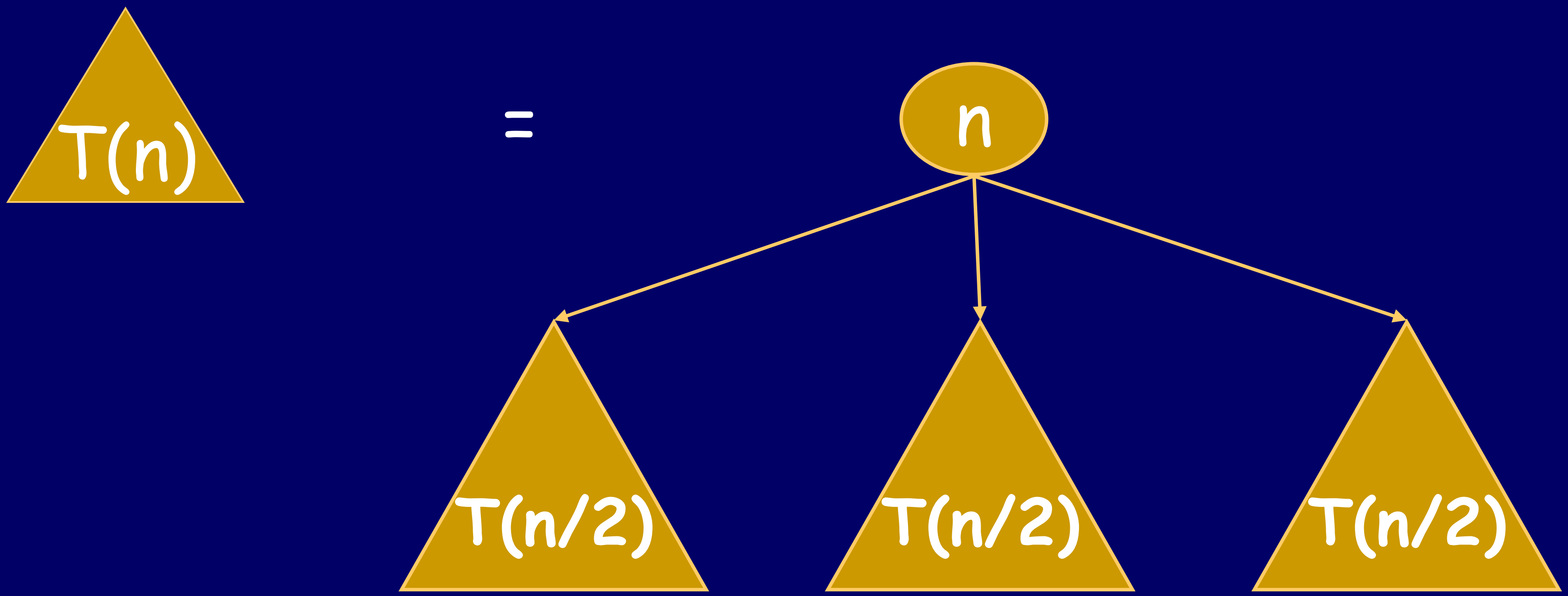
$X \times Y = z2\,2^{n} + z5\,2^{n/2} + z3$

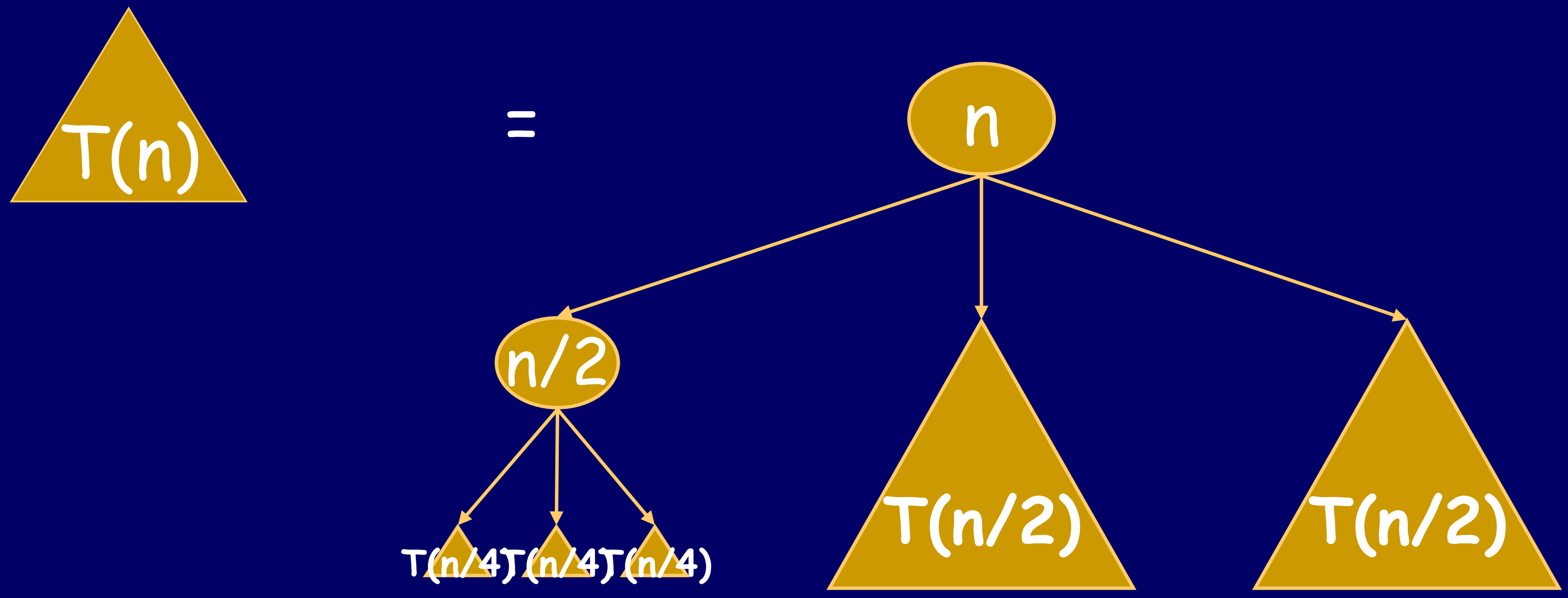
Karatsuba (1962)

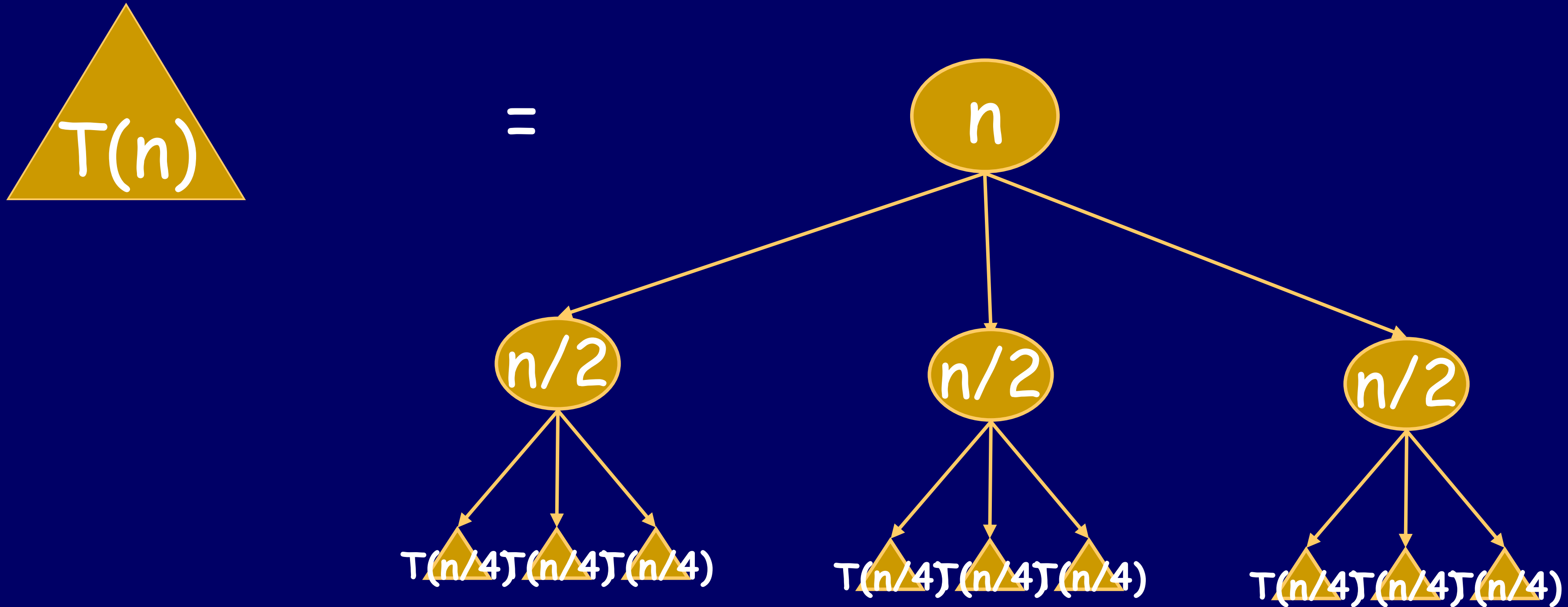
$$T(1) = 1$$

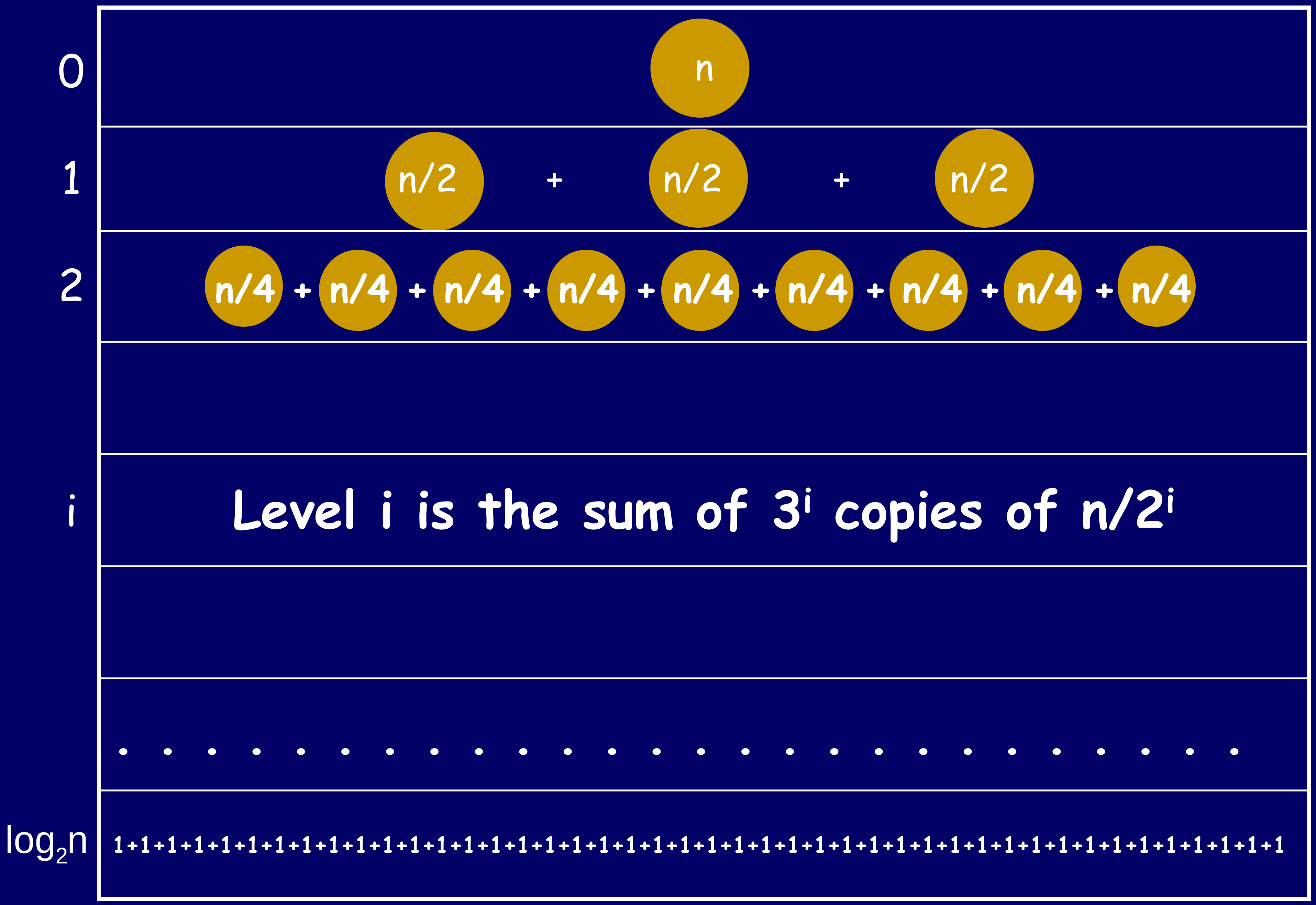
$$T(n) = 3\,T(n/2) + n$$

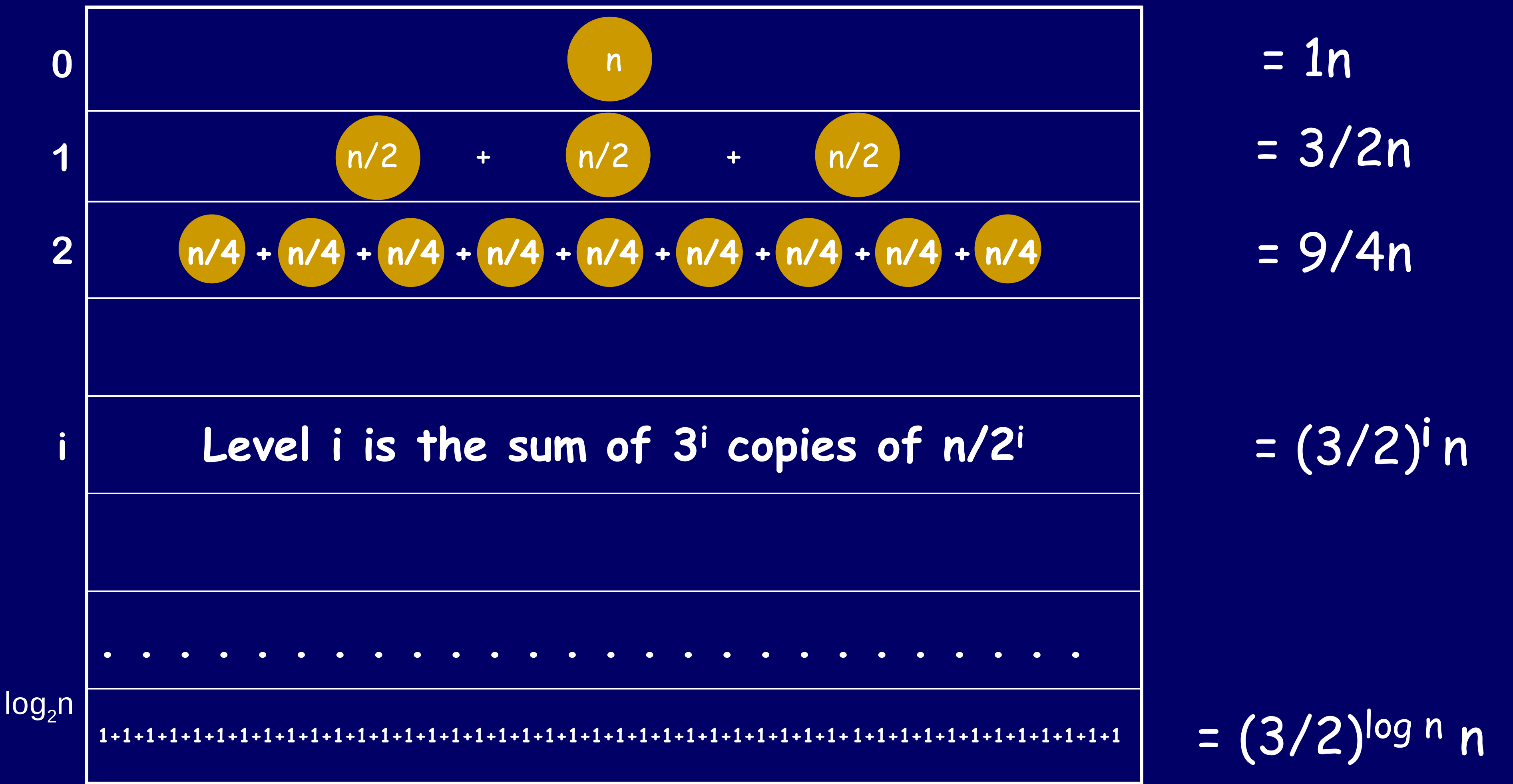
What is the growth rate of T(n)?


T(n)
=
n
T(n/2)
T(n/2)
T(n/2)


T(n)
=
n
n/2
T(n/2)
T(n/2)
T(n/4)
T(n/4)
T(n/4)


T(n)
=
n
n/2
n/2
n/2
T(n/4)T(n/4)T(n/4)
T(n/4)T(n/4)T(n/4)
T(n/4)T(n/4)T(n/4)


0
n
1
n/2
+
n/2
+
n/2
2
n/4 + n/4 + n/4 + n/4 + n/4 + n/4 + n/4 + n/4 + n/4
i
Level i is the sum of 3^i copies of $n/2^i$
. . . .
$\log_2 n$
1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1



$$T(n) = n\,(1 + 3/2 + (3/2)^2 + \ldots + (3/2)^{\log_2 n}) \quad = \quad ??$$

The Geometric Series

$$1 + X^1 + X^2 + X^3 + \ldots + X^{k-1} + X^k = \frac{X^{k+1} - 1}{X - 1}$$

We have: $X = 3/2$ $\qquad$ $k = \log_2 n$

$$\frac{(3/2) \times (3/2)^{\log_2 n} - 1}{\frac{1}{2}} = 3 \times (3^{\log_2 n}/2^{\log_2 n}) - 2$$

$$= 3 \times (3^{\log_2 n}/n) - 2$$

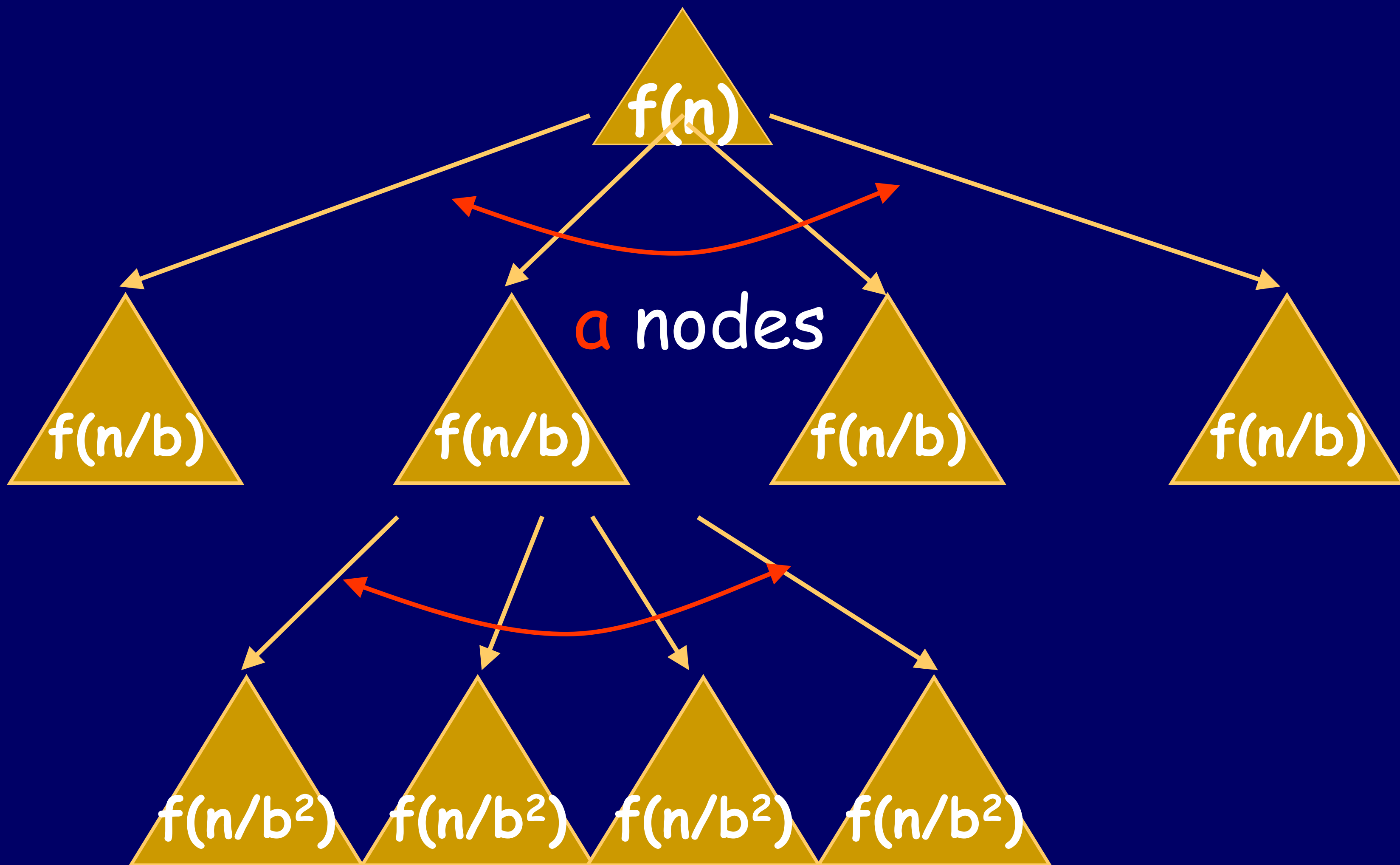
Dramatic improvement for large n

$T(n) = 3\, n^{\log_2 3} - 2n = \Theta(n^{\log_2 3}) = \Theta(n^{1.58\ldots})$

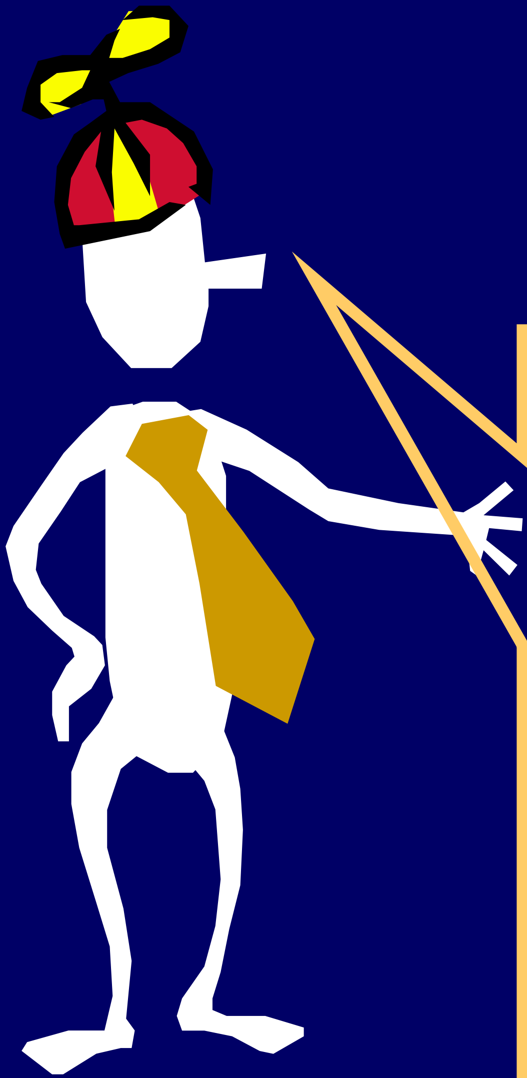
A huge savings over $\Theta(n^2)$ when n gets large.

Recursion Tree Representation

$$T(n) = a\,T(n/b) + f(n)$$



Exercise



Solve the following recurrence

$$T(n) = p\,T(n/3) + n$$

where $p>0$.

$$T(n) = p\, T(n/3) + n$$

Let p>3 be an arbitrary parameter.

Using the tree method, we obtain

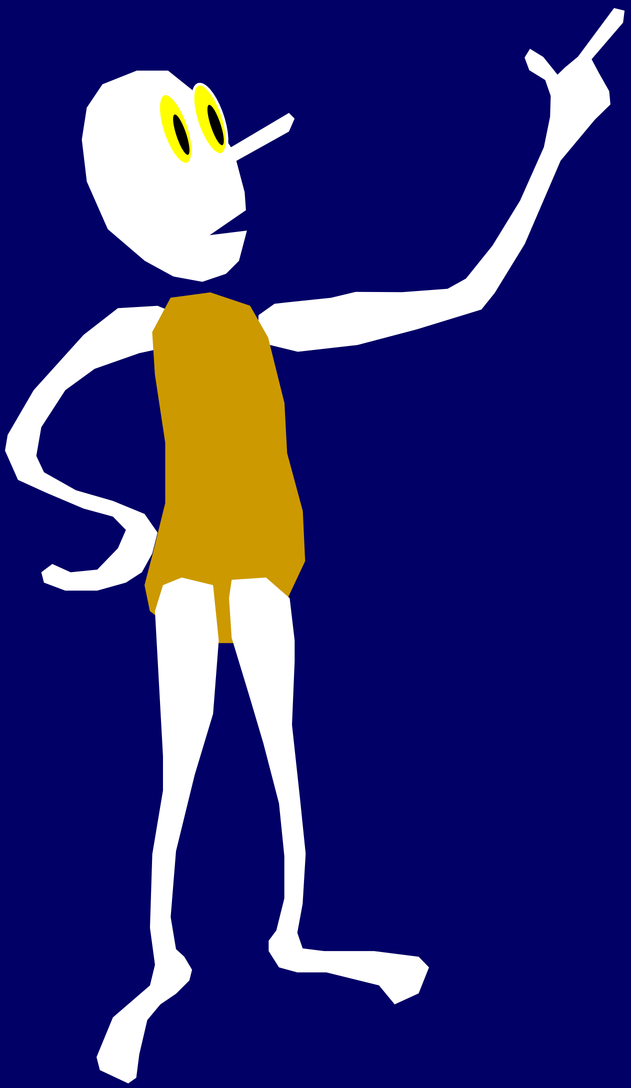
$$T(n) = n(1 + p/3 + p^2/9 + \ldots + (p/3)^h)$$

where the tree height is $\log_3 n$.

It follows

$$T(n) = \Theta(n^{\log_3 p})$$

Recurrence

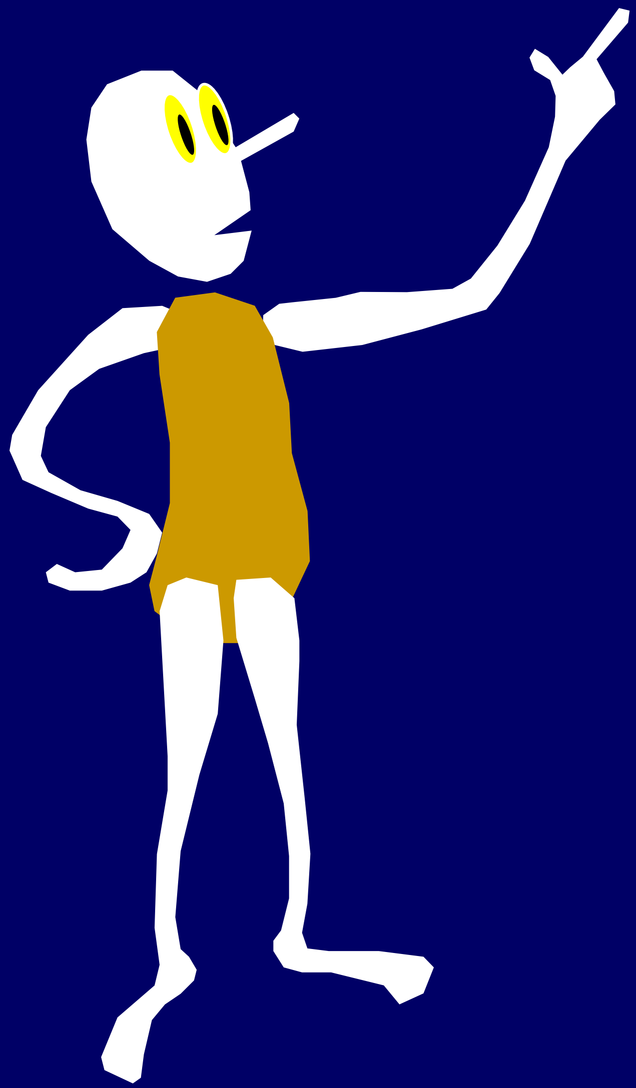


$$T(n) = p\,T(n/3) + n$$

has the following asymptotic solution

$$T(n) = \Theta\left(n^{\log_3 p}\right)$$

when $p>3$.



$$T(n) = p\ T(n/3) + n$$

Cases p =1, 2 and 3 should be considered separately

If p =3, then

$$T(n) = \Theta\ (n \log n)$$

3-Way Multiplication

$$X = a_1\, 2^{n/4} + a_2\, 2^{n/2} + a_3$$

$$Y = b_1\, 2^{n/4} + b_2\, 2^{n/2} + b_3$$

$$T(1) = 1$$

$$T(n) = 9\, T(n/3) + n$$

3-Way Multiplication

$$T(n) = p\,T(n/3) + n$$

$$T(n) = \Theta(n^{\log_3 p})$$

To get an improvement over Karatsuba's, we have to decrease the number of multiplications to at least 5.

Toom and Cook (1963, 1966)

$$T(1) = 1$$

$$T(n) = 5\,T(n/3) + n$$

$$T(n) = \Theta(n^{\log_3 5}) = \Theta(n^{1.46\ldots})$$

3-Way Multiplication

$$X = a_1\, 2^{n/4} + a_2\, 2^{n/2} + a_3$$

$$Y = b_1\, 2^{n/4} + b_2\, 2^{n/2} + b_3$$

Is it possible to reduce the number of multiplications to 5?

Multiplication Algorithms

Grade School	n^2
Karatsuba	$n^{1.58...}$
3-way	$n^{1.46...}$
FFT	$n \log^2 n$
Schönhage and Strassen	$n \log n \log\log n$