Synthesis, Analysis, and Verification

Lecture 08

BAPA: Quantifier Elimination and Decision Procedures

WS1S: Automata-Based Decision Procedure

Lectures:

Viktor Kuncak

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Boolean Algebra with Presburger Arithmetic

$$
\begin{array}{lcl}
F & ::= & A \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \neg F \mid \exists x.F \mid \forall x.F \mid \exists k.F \mid \forall k.F \\
A & ::= & B_1 = B_2 \mid B_1 \subseteq B_2 \mid T_1 = T_2 \mid T_1 < T_2 \mid (K|T) \\
B & ::= & x \mid \mathbf{0} \mid \mathbf{1} \mid B_1 \cup B_2 \mid B_1 \cap B_2 \mid B^c \\
T & ::= & k \mid K \mid maxc \mid T_1 + T_2 \mid K \cdot T \mid \ |B| \\
K & ::= & \ldots -2 \mid -1 \mid 0 \mid 1 \mid 2 \ldots
\end{array}
$$

Quantifier Elimination

Usually harder than just satisfiability checking

High-level idea:

- express everything using cardinalities
- separate integer arithmetic and set part
  (using auxiliary integer variables)
- reduce set quantifier to integer quantifier
- eliminate integer quantifier
- eliminate auxiliary integer variables

Eliminate Quantifier

$\exists B.\ A \subseteq B \wedge B \subset C \longrightarrow F(A, C)$

$A \subset C$?

$|A \cap B^c| = 0 \wedge |B \cap C^c| = 0 \wedge |C \cap B^c| \geq 1$

$k_0 = |A^c \cap B^c \cap C^c|$

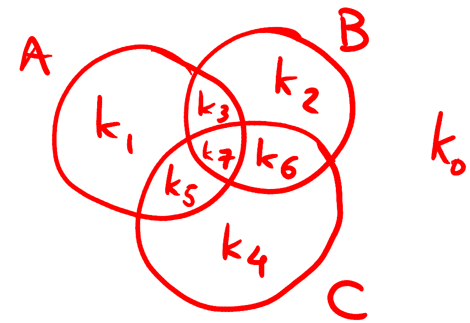
$k_1 = |A \cap B^c \cap C^c|$

$\vdots$

$k_7 = |A \cap B \cap C|$

$|A \cap C^c| = 0 \wedge |A^c \cap C| \geq 1$

$\boxed{\begin{array}{l} \ell_1 = 0 \\ \ell_2 \geq 1 \end{array}}$



$|A \cap B^c| = k_1 + k_5$

$\boxed{k_1 + k_5 = 0}$

$|B \cap C^c| = k_2 + k_3$

$\boxed{k_2 + k_3 = 0}$

$|C \cap B^c| = k_4 + k_5$

$\boxed{k_4 + k_5 \geq 1}$

$|A \cap B \cap C^c| = k_3$

$|A \cap B^c \cap C^c| = k_1$

$\downarrow\ |A \cap C^c| = k_1 + k_3$

$\exists B.$

$|A \cap B \cap C| = k_7$

$|A \cap B^c \cap C| = k_5$

$\updownarrow$

$|A \cap C| = k_5 + k_7$

$\boxed{\begin{array}{l} \ell_1 = k_1 + k_3 \\ \ell_2 = k_4 + k_6 \end{array}}$

$|A \cap C| = \ell_3$

$|A \cap C^c| = \ell_1$

$\boxed{\ell_3 = k_5 + k_7}$

$|A^c \cap C| = \ell_2$

$$\exists k_1, k_2, \dots, k_7, k_0 . \quad \bigwedge_{i=0}^{7} k_i \geq 0$$

$$k_1 + k_5 = 0 \ \wedge \ k_2 + k_3 = 0 \ \wedge \ k_4 + k_5 \geq 1 \ \wedge$$

$$\ell_0 = k_0 + k_2 \ \wedge \ \ell_1 = k_1 + k_3 \ \wedge \ \ell_2 = k_4 + k_6 \ \wedge$$

$$\ell_3 = k_5 + k_7$$

$$1, 2, 3, 5 \longrightarrow 0$$

$$k_4 \geq 1 \ \wedge$$

$$\cancel{\ell_0 = k_0} \ \wedge \ \ell_1 = 0 \ \wedge \ \boxed{\ell_2 = k_4 + k_6} \ \wedge$$

$$\cancel{\ell_3 = k_7}$$

$$k_6 = \ell_2 - k_4$$

$$\exists k_4 . \quad \ell_2 - k_4 \geq 0 \ \wedge$$

$$k_4 \geq 1 \quad \wedge$$

$$\boxed{\ell_1 = 0}$$

$$1 \leq k_4$$

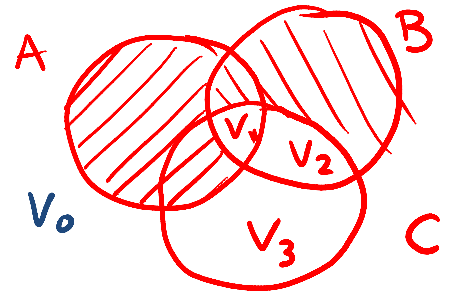
$$k_4 \leq \ell_2$$

$$\boxed{1 \leq \ell_2}$$

Eliminate Quantifier

$$\exists B.\ \ A \subseteq B \ \wedge\ B \subset C$$

$$|A\cap B^c|=0 \ \wedge\ |B\cap C^c|=0 \ \wedge\ \boxed{|C\cap B^c|\geq 1}$$



$V_1 = A\cap B\cap C$

$V_2 = A^c\cap B\cap C$

$V_3 = A^c\cap B^c\cap C$

$C = V_1 \uplus V_2 \uplus V_3$

$B = V_1 \uplus V_2$

$C \cap B^c = V_1 \uplus V_2$

$A = V_1$

V_1, V_2, V_3 - disjoint

$\exists k_1.\ k_1 = |V_1| \qquad \exists k_2.\ k_2 = |V_2| \qquad \exists k_3.\ k_3 = |V_3| \qquad \exists k_0.\ k_0 = |V_0|$

$|A\cap B\cap C| = k_1 \ \wedge\ |A\cap B^c\cap C| = 0 \ \rightsquigarrow\ |A\cap C| = k_1$

$|A\cap B\cap C^c| = 0 \ \wedge\ |A\cap B^c\cap C^c| = 0 \ \rightsquigarrow\ |A\cap C^c| = 0$

$|A^c\cap B\cap C| = k_2 \ \wedge\ |A^c\cap B^c\cap C| = k_3 \ \rightsquigarrow\ |A^c\cap C| = k_3$

$|A^c\cap B\cap C^c| = 0 \ \wedge\ |A^c\cap B^c\cap C^c| = k_0 \ \rightsquigarrow\ |A^c\cap C^c| = k_0$

$|A\cap C\cap B^c| + |A^c\cap C\cap B^c| \geq 1 \qquad k_3 \geq 1$

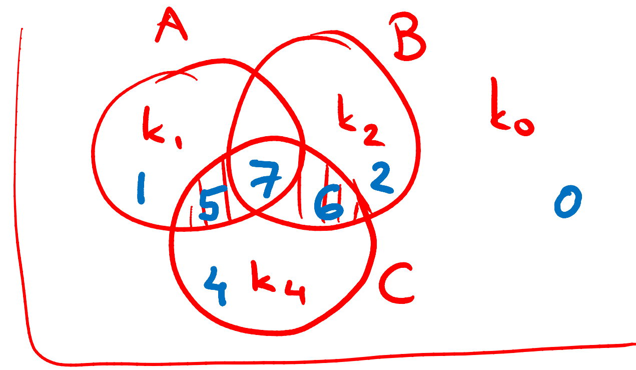
$$|A\cap C^c|=0 \ \wedge\ |A^c\cap C|\geq 1$$

$$A \subseteq C \ \wedge\ |C\setminus A| \geq 1$$

Eliminate Quantifier

$\forall C. \quad A \cap C \neq \emptyset \;\vee\; B \cap C \neq \emptyset$

Eliminate Quantifier



$\forall C.\quad A\cap C \neq \emptyset \;\vee\; B\cap C \neq \emptyset$

$\neg\exists C.\quad A\cap C = \emptyset \;\wedge\; B\cap C = \emptyset$

$|A\cap C| = 0 \;\wedge\; |B\cap C| = 0$

$\neg\exists k_1,k_2,k_3,k_4,k_5,k_6,k_7,k_0.\ \exists C.$

$k_1 = |A\cap B^c \cap C^c|$

$k_2 = |A^c\cap B\cap C^c|$

$\vdots$

$k_5 = k_{1+4} = |\underset{1}{A}\cap B^c \cap \underset{4}{C}|$

$k_6 = k_{2+4} = |A^c \cap \underset{2}{B} \cap \underset{4}{C}| \quad \wedge$

$|A\cap C| = |A\cap B^c\cap C| + |A\cap B\cap C|$

$= k_5 + k_7$

$|B\cap C| = k_6 + k_7$

$k_5 + k_7 = 0 \quad\wedge\quad k_6 + k_7 = 0$

$\neg\exists k_0, k_1,\dots,k_7.\quad |A\cap B| = k_3 + k_7$

$\ell_3 \quad |A\cap B^c| = k_1 + k_5$

$\ell_2 \quad |A^c\cap B| = k_2 + k_6$

$\ell_1 \quad |A^c\cap B^c| = k_4 + k_0 \quad \wedge\ k_5 + k_7 = 0 \ \wedge\ k_6 + k_7 = 0$

ℓ_0

$\neg\exists\, \ell_0^{\geq 0}, \ell_1, \ell_2, \ell_3^{\geq 0}.\ \exists k_0^{\geq 0},\dots,k_7^{\geq 0}.$ $\rightarrow P'(\vec{\ell})$

$\ell_0 = |A^c\cap B^c| \wedge \dots \wedge \ell_3 = |A\cap B| \wedge \quad P(\ell_0,\ell_1,\ell_2,\ell_3,k_0,k_1,\dots,k_7)$

Eliminate Quantifier

$\forall C. \quad A \cap C \neq \emptyset \ \vee \ B \cap C \neq \emptyset$

$\neg \exists \ell_0, \ell_1, \ell_2, \ell_3 . \quad \ell_0 = |A^c \cap B^c|$
$\ell_1 = |A \cap B^c|$
$\ell_2 = |A^c \cap B|$
$\ell_3 = |A \cap B| \ \wedge$
$P'(\ell_0, \ell_1, \ell_2, \ell_3)$

$\neg \ P'(\ |A^c \cap B^c|, |A \cap B^c|, |A^c \cap B|, |A \cap B|\ )$

Another Example

$\exists A, B.$
$A \cup B = S \wedge |A \cap B| = 0 \wedge |A| = |B|$

Quantifier-free Boolean Algebra with Presburger Arithmetic (QFBAPA)

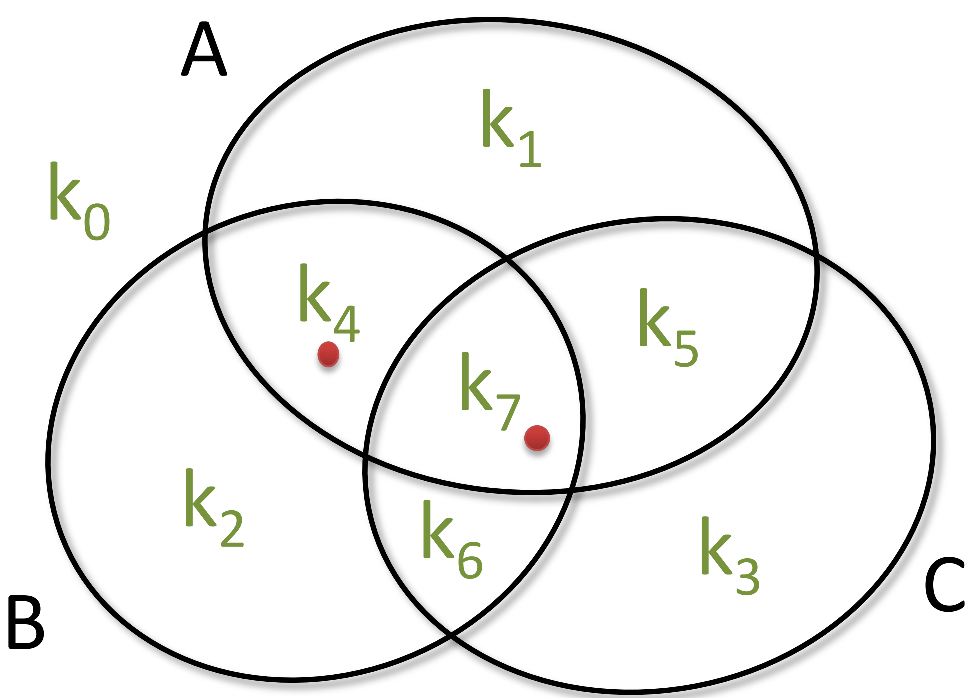
$$\phi ::= \phi \vee \phi, \quad \phi \wedge \phi, \quad \neg \phi, \quad A$$
$$A ::= S = S, \quad S \subseteq S, \quad T = T, \quad T \leq T$$
$$S ::= s_i, \quad \emptyset, \quad S \cup S, \quad S \cap S, \quad S \setminus S$$
$$T ::= k_i, \quad c, \quad c \cdot T, \quad T + T, \quad T - T, \quad |S|$$
$$c ::= \ldots, \; -2, \; -1, \; 0, \; 1, \; 2, \; \ldots$$

- If sets are over integers:

$$A ::= \ldots, \quad T \in S$$
$$S ::= \ldots, \quad \{ T \}$$

A Decision Procedure for QFBAPA

$$| A | > 1 \ \land \ A \subseteq B \ \land \ | B \cap C | \leq 2$$



$$\overbrace{k_1 + k_4 + k_5 + k_7}^{=\ell_1} > 1$$

$$\overbrace{k_1 + k_5}^{=\ell_2} = 0$$

$$\overbrace{k_6 + k_7}^{=\ell_3} \leq 2$$

$$\forall i \in \{0, \ldots, 7\}.\ k_i \geq 0$$

$$\downarrow$$

$$\ell_1 > 1 \land \ell_2 = 0 \land \ell_3 \leq 2$$

$$k_4 = k_7 = 1$$

$$\forall i \notin \{4, 7\}.\ k_i = 0$$

$$\downarrow$$

$$A = \{1, 2\},\ B = \{1, 2\},\ C = \{2\}$$

A Decision Procedure for QFBAPA

- Simple proof of decidability.
- Very simple linear arithmetic constraints, but…
- …for *n* set variables, uses 2^n integer variables
- Two orthogonal ways to improve it
  - sparse solutions
  - identifying independent constraints

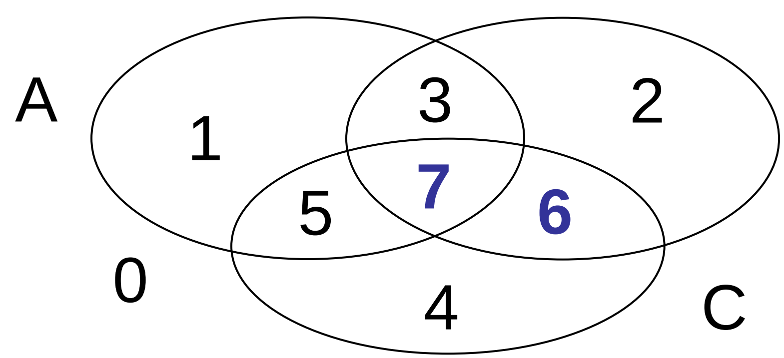
Sparse Solutions

The difficulty of the general problem reduces to

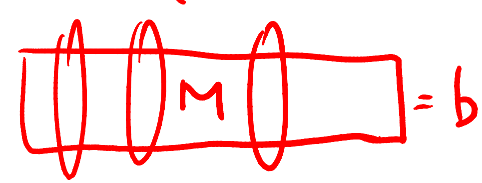
integer linear programming problems
with many integer variables
but still polynomially many constraints.

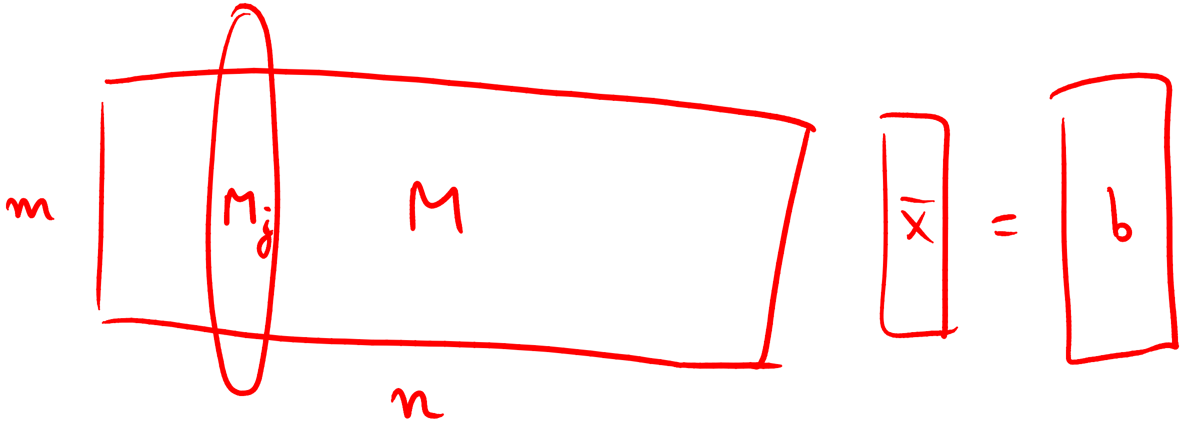
$\mathrm{card}(A \cup B) = k_1$ $\mathrm{card}(B \cap C) = k_2$

$x_1 + x_2 + x_3 + x_5 + x_6 + x_7 = k_1$ $\mathbf{x_6 + x_7 = k_2}$



$M x = \vec{b}$





$\bar{x} \in \mathbb{R}^n$

$n \gg m$

$$\sum_{j=1}^{n} x_j \bar{M}_j = b$$

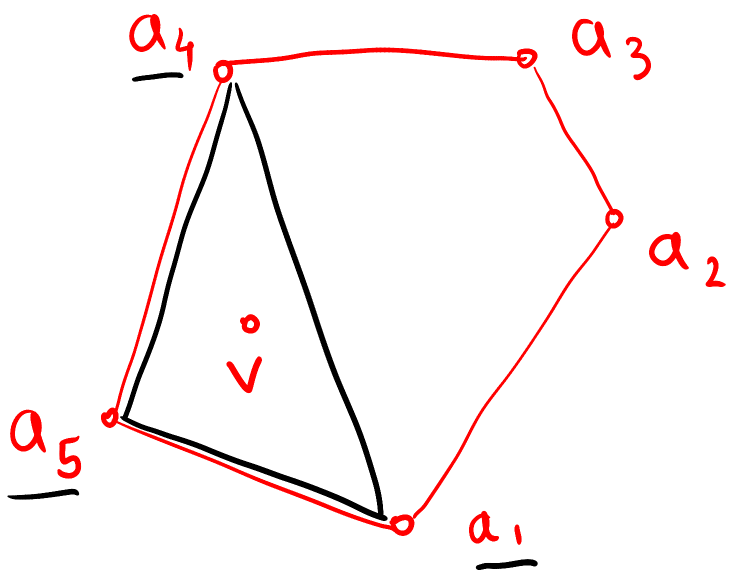
what if

$x_j \geq 0$

Caratheodory theorem

Vector v of dimension d

is a convex combination of { a_1 , … , a_n }



$\sum \lambda_i \bar{a}_i = v$

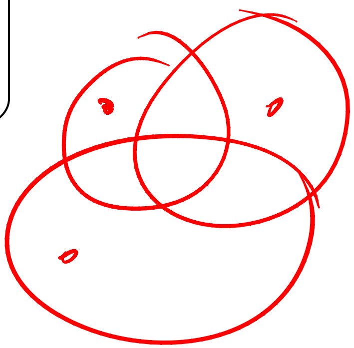
$\lambda_i \geq 0 \quad \sum \lambda_i = 1$

Then it is a convex combination of a subset { $a_{k(1)}$, … , $a_{k(d+1)}$ } of (d+1) of them

ILP associated w/ formula of size n

Integer linear programming problem: for non-negative x_i

$$\left.\underbrace{\begin{array}{l} x_1 + x_2 + x_3 + x_5 + x_6 + x_7 = p \\ \quad \ldots \\ x_6 + x_7 = q \end{array}}_{2^n \text{ variables}}\right\} n \text{ equations}$$



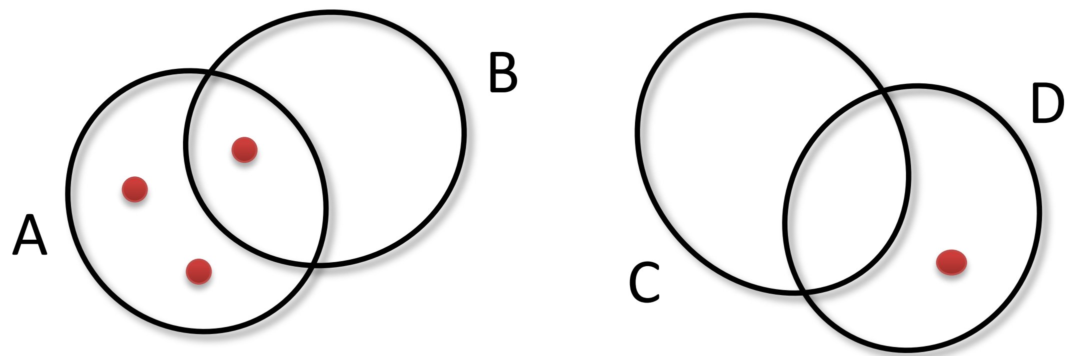
Are there **sparse** solutions where $O(n^k)$ variables are non-zero?

- for reals - yes, matrix rank is $O(n)$
- for non-negative reals - yes, Caratheodory them
- for non-negative integers **- Eisenbrand, Shmonin'06**

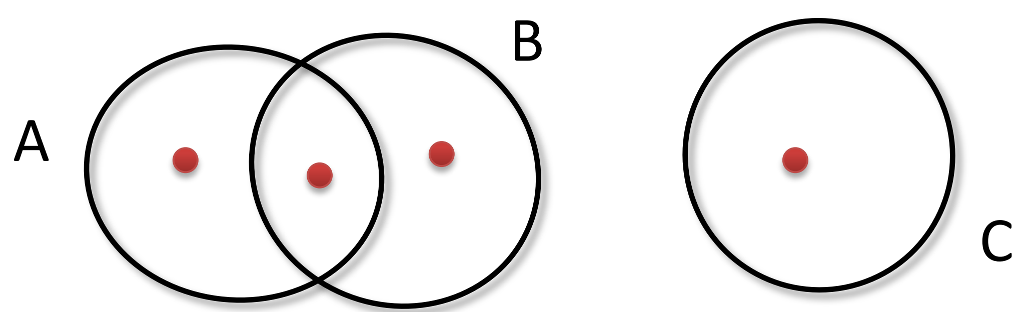
Integer Caratheodory thm. (only when coefficients are bounded)

Independent Constraints

$| A \cup B | = 3 \ \wedge \ C \subseteq D$



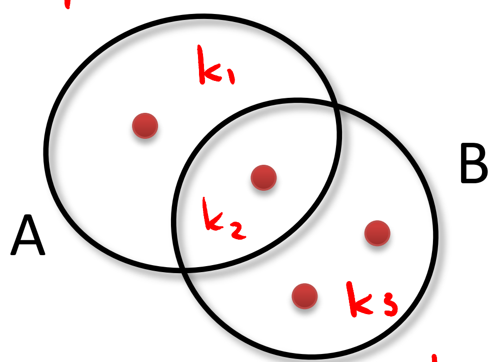
$| A \setminus B | = | C |$

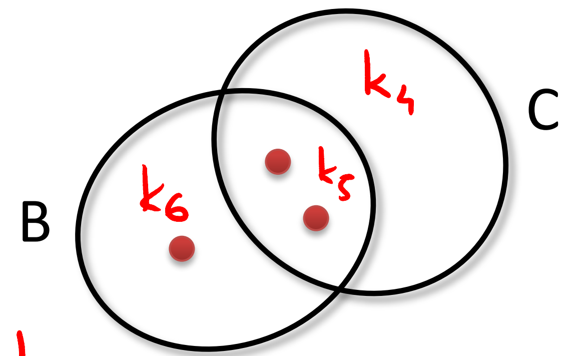


Independent Constraints

$$|A \cup B| = 4 \wedge |B \cap C| = 2$$

$k_1 + k_2 + k_3 = 4$ $\wedge$ $k_5 = 2$



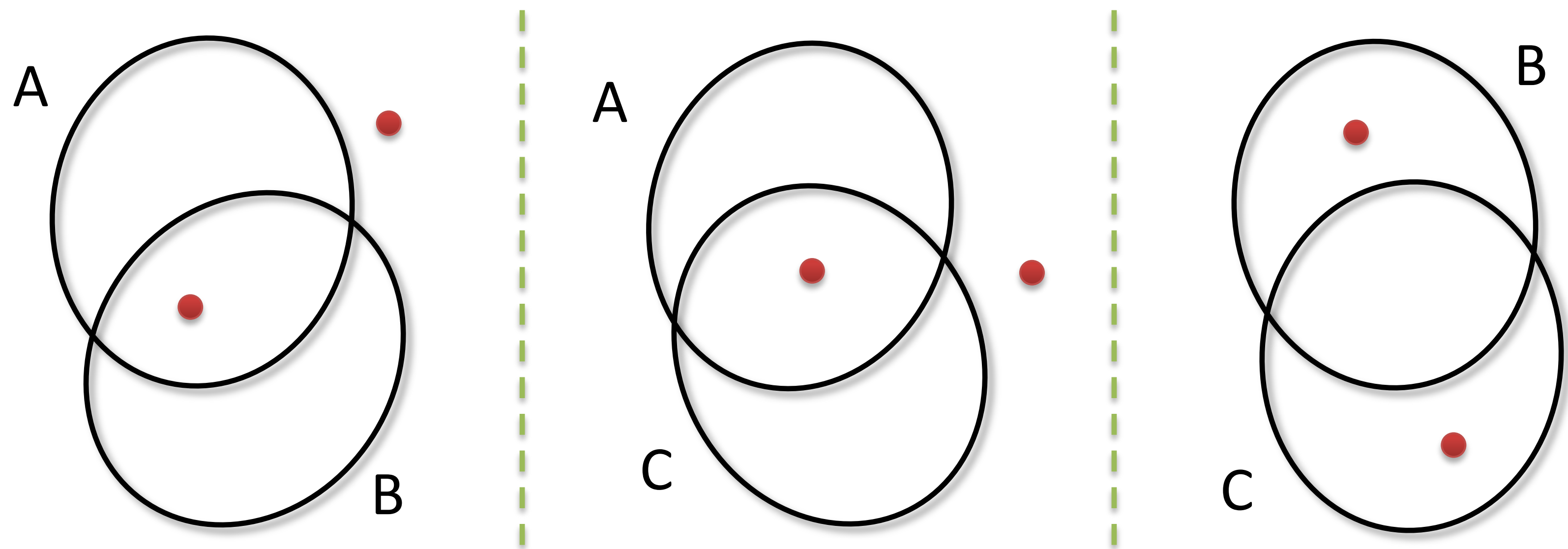


$k_2 + k_3 = k_5 + k_6$

- A and C are only indirectly related.
- All that matters is that the models for B are compatible.

When can Models be Combined?

$$|A| = 1 \ \wedge \ |B| = 1 \ \wedge \ |A \cap B| = 1$$
$$\wedge \ |A| = 1 \ \wedge \ |C| = 1 \ \wedge \ |A \cap C| = 1$$
$$\wedge \ |B| = 1 \ \wedge \ |C| = 1 \ \wedge \ |B \cap C| = 0$$



The models are pairwise compatible, yet cannot be combined.

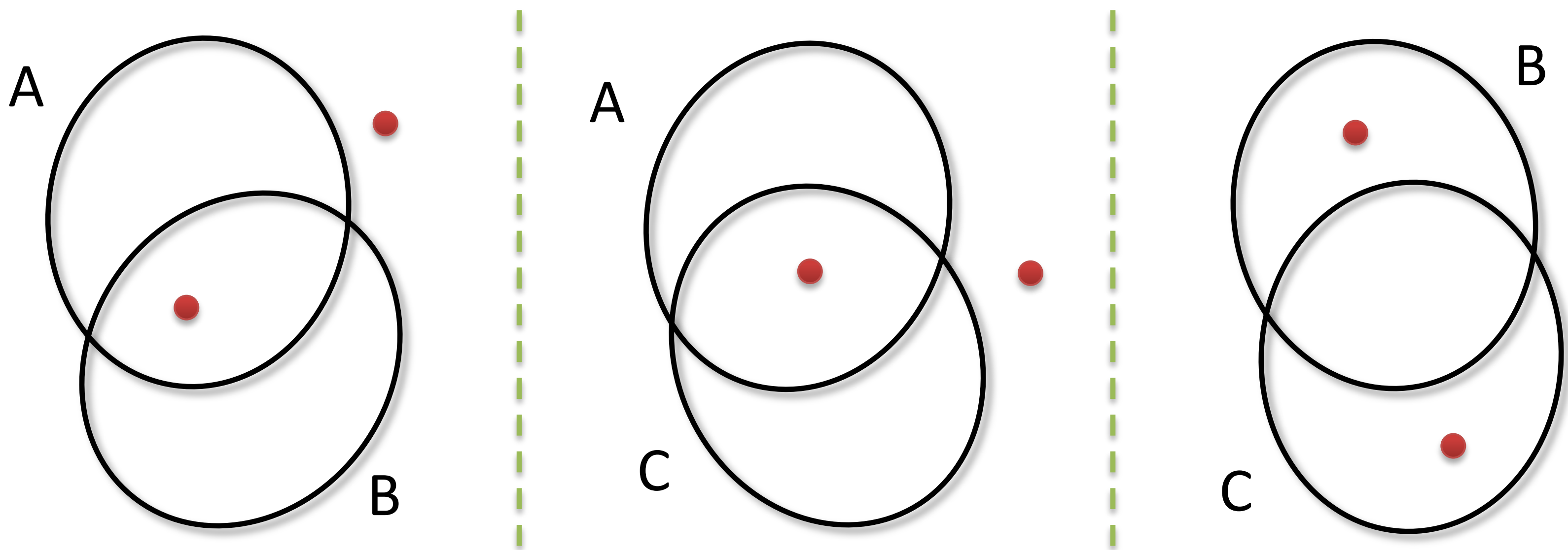
When can Models be Combined?

Theorem 3

- Let $\varphi_1, \ldots, \varphi_n$ be BAPA constraints.
- Let **V** be the set of all set variables that appear in at least two constraints.
- Models $M_1, \ldots, M_n$ for $\varphi_1, \ldots, \varphi_n$ can be combined into a model M for $\varphi_1 \wedge \ldots \wedge \varphi_n$ if and only if they "agree" on the sizes of all Venn regions of the variables in **V**.

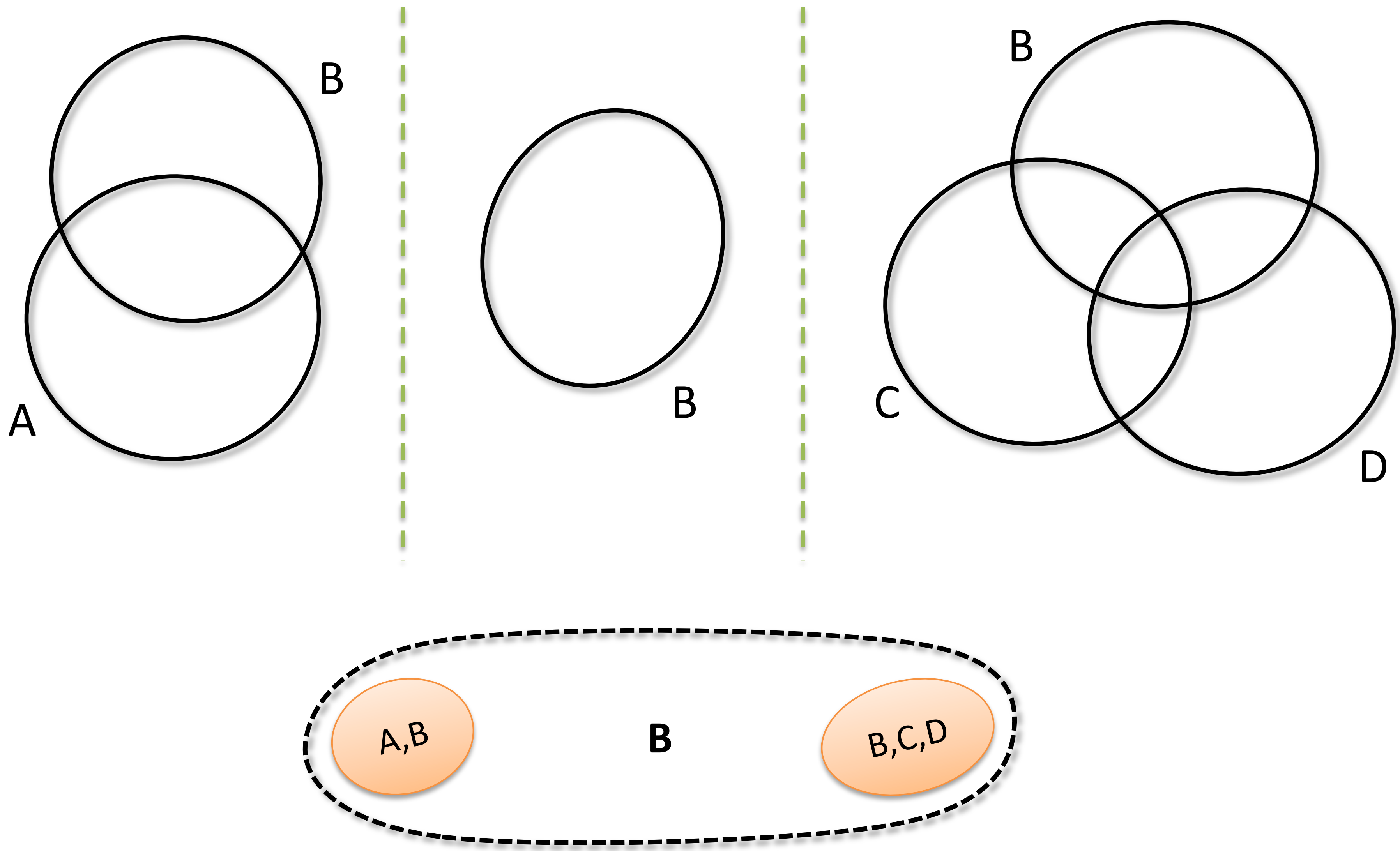
When can Models be Combined?

$$|A| = 1 \land |B| = 1 \land |A \cap B| = 1$$
$$\land\ |A| = 1 \land |C| = 1 \land |A \cap C| = 1$$
$$\land\ |B| = 1 \land |C| = 1 \land |B \cap C| = 0$$

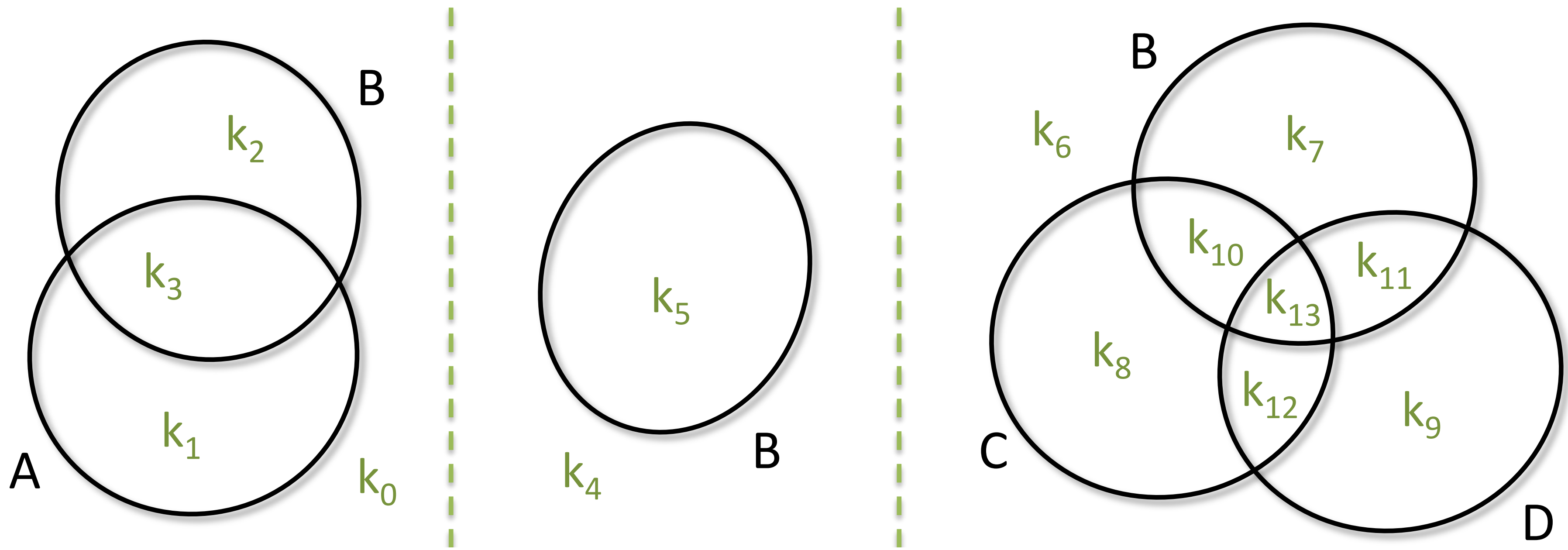


V = { A, B, C } and models don't agree on $|A \cap B \cap C|$.

$$|A \setminus B| > |A \cap B| \wedge B \cap C \cap D = \emptyset \wedge |B \setminus D| > |B \setminus C|$$



$$|A \setminus B| > |A \cap B| \wedge B \cap C \cap D = \emptyset \wedge |B \setminus D| > |B \setminus C|$$



$$k_0 + k_1 = k_4 \qquad k_4 = k_6 + k_8 + k_9 + k_{12}$$

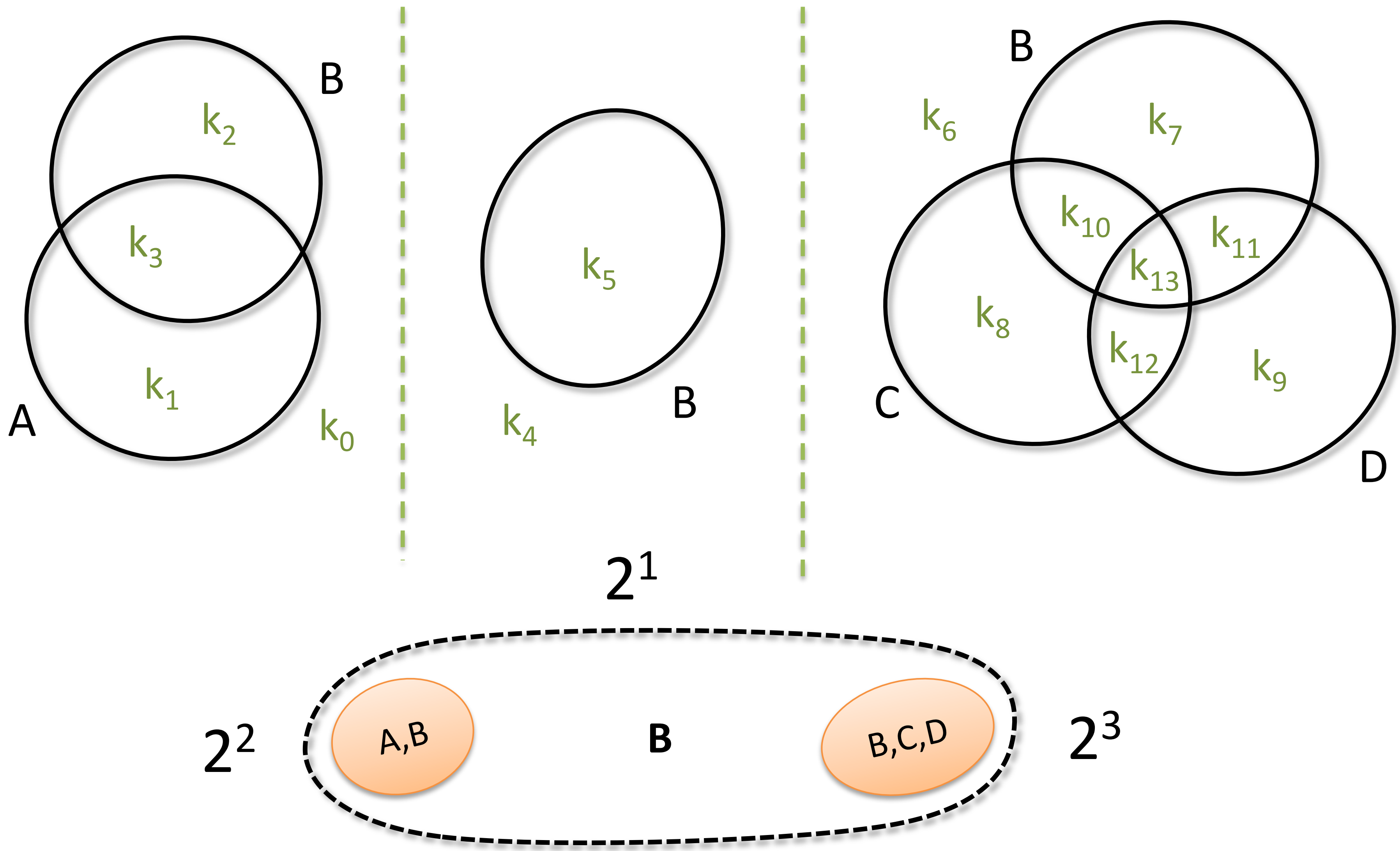
$$k_2 + k_3 = k_5 \qquad k_5 = k_7 + k_{10} + k_{11} + k_{13}$$

A,B

B,C,D

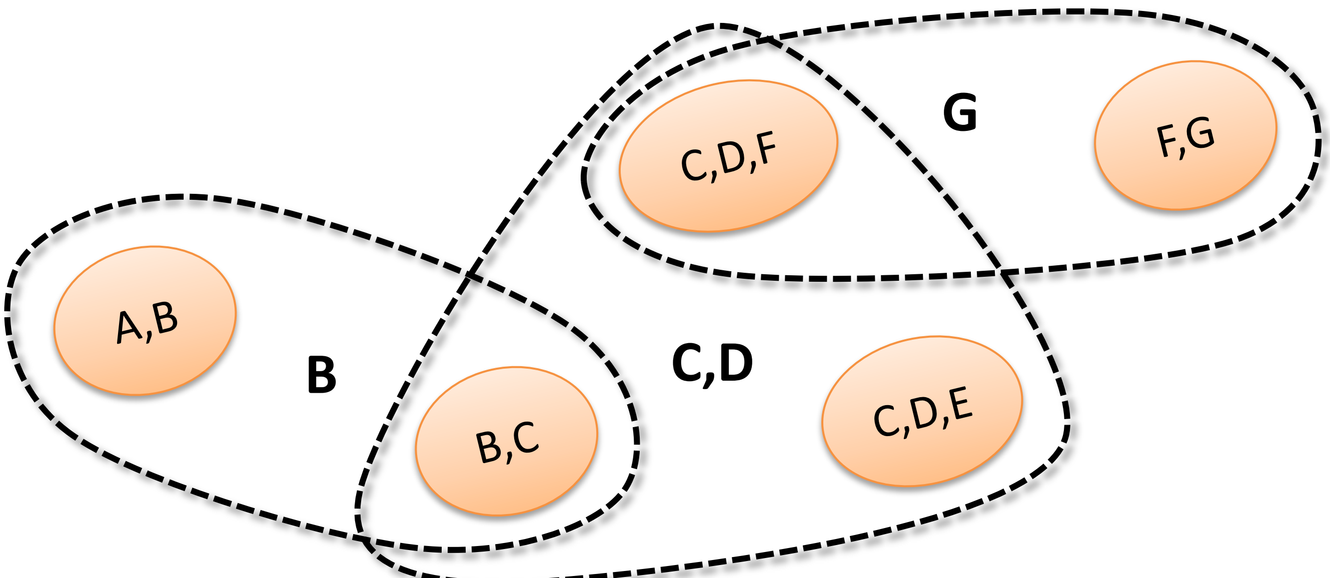
$$\longrightarrow \quad k_1 > k_3 \wedge k_{13} = 0^{\mathbf{B}} \wedge k_7 + k_{10} > k_7 + k_{11}$$

$$|A \setminus B| > |A \cap B| \wedge B \cap C \cap D = \emptyset \wedge |B \setminus D| > |B \setminus C|$$



Hypertree Decomposition

$$|A \cup B| \leq 3 \wedge C \subseteq B \wedge |(C \cap D) \setminus E| = 2$$
$$\wedge\ |(C \cap F) \setminus D| = 2 \wedge G \subseteq F$$



- Hyperedges correspond to applications of Theorem 3.

Functional Programs: Example

- Given:

```
def content(lst: List[Int]) : Set[Int] = lst match {
  case Nil ⇒ ∅
  case Cons(x, xs) ⇒ { x } ∪ content(xs)
}
```

```
def length(lst : List[Int]) : Int = lst match {
  case Nil ⇒ 0
  case Cons(x, xs) ⇒ 1 + length(xs)
}
```

- We want to prove:

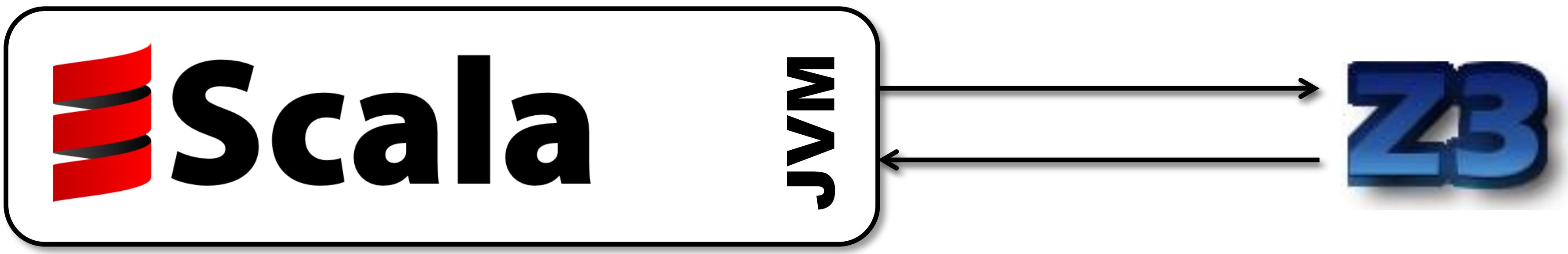
$$\forall\ list : List[Int]\ .\ |\ content(list)\ | \leq length(list)$$

- SMT query:

$$\begin{aligned}
& length(list) > |\ content(list)\ | \\
& \wedge\ content(Nil) = \emptyset \\
& \wedge\ \forall\ x{:}\ Int,\ \forall\ xs{:}\ List[Int] : content(Cons(x, xs)) = \{ x \} \cup content(xs) \\
& \wedge\ length(Nil) = 0 \\
& \wedge\ \forall\ x{:}\ Int,\ \forall\ xs{:}\ List[Int] : length(Cons(x, xs)) = 1 + length(xs)
\end{aligned}$$

System Architecture

- Maintains the hypertree decomposition
- Translates constraints on sets to constraints on integers
- Lifts integer model to model for sets



- Reasons about all other theories
- Communicates new BAPA constraints
- Notifies when push/pop occurs

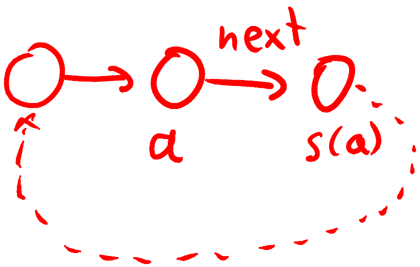
WS1S

- Weak Monadic Second-Order Logic of One Successor

  $$F ::= v \subseteq v \mid succ(v, v) \mid F \vee F \mid \neg F \mid \exists v.F$$

- Like BAPA, allows quantification over sets
- Unlike BAPA, does not allow |A|=|B|
- However, it allows talking about lists
  - BAPA talks only about identities of elements
  - (There is a way to combine WS1S and BAPA)
- WS1S generalizes to WSkS – reachability in trees!

A Verification Condition in WS1S



$\{\, noCycles(next) \,\}$

$p.next = q$

$\{\, noCycles(next) \,\}$

$next' = next\,(p := q)$

$noCycles(next) \wedge next' = next(p := q) \wedge \neg noCycles(next')$

next is successor

$\exists a \quad (\, s(a), a) \in \{(x,y) \mid \overbrace{y = next'(x) \wedge x \neq null \wedge y \neq null}^{T}\}^*$

$(x \neq p \wedge y = s(x)) \vee (x = p \wedge y = q)$

$\forall R. \quad s(a) \in R \wedge \underbrace{(\forall x,y.\ x \in R \wedge T(x,y) \rightarrow y \in R)}_{closed_T(R)}$

$\rightarrow \quad a \in R$