Using the temporal monodic clique-guarded negation fragment to specify swarm properties

Sen Zheng, Michael Fisher, and Clare Dixon

August 8, 2023

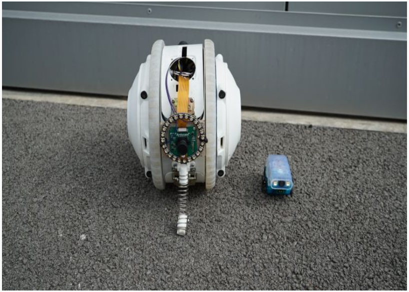
The University of Manchester

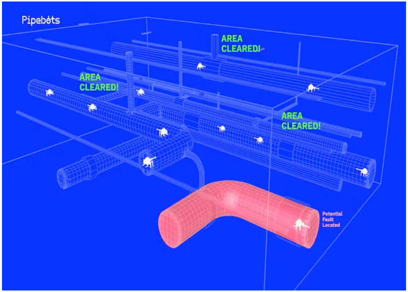
First-order Modal and Temporal Logics (FOMTL2023)

Robotic Swarm is Useful

- Swarm sensing forest fire

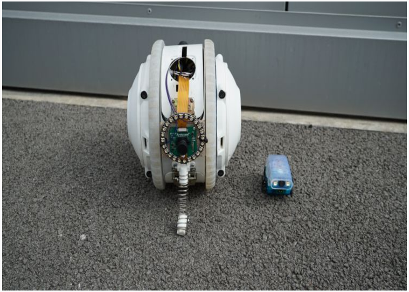
Robotic Swarm is Useful



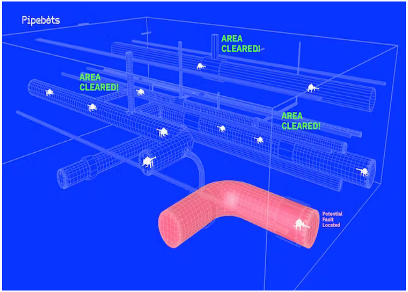


- Swarm sensing forest fire
- Pipebots testing buried pipe network

Robotic Swarm is Useful



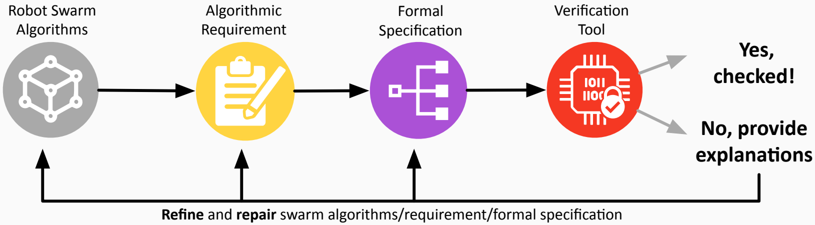
- Swarm sensing forest fire
- Pipebots testing buried pipe network



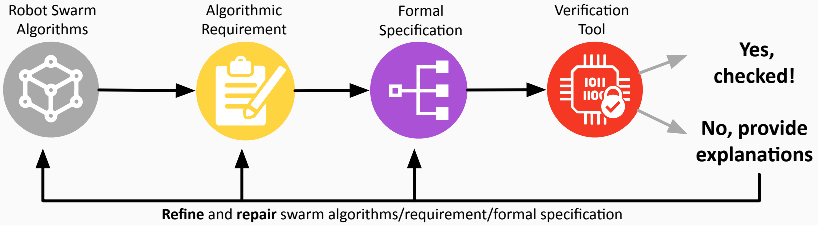
Not (always) reliable!

Our Proposal to Verify Swarms

Our Proposal to Verify Swarms



Our Proposal to Verify Swarms



1. Identifying **algorithms** and eliciting **requirement**
2. **Formalisation** of 1. in **first-order temporal logic**
3. **Deductive reasoning** procedures and tools
4. **Refine** and **repair** 1. and 2.

Why MCGNF for Swarm Verification

2. Formalisation of 1. in **first-order temporal logic**

Why MCGNF for Swarm Verification

2. Formalisation of 1. in **first-order temporal logic**

Temporal Monodic Clique-Guarded Negation Fragment (MGCNF)

Why MCGNF for Swarm Verification

2. Formalisation of 1. in first-order temporal logic

Temporal **Monodic** Clique-Guarded Negation Fragment (MGCNF)

Why MCGNF for Swarm Verification

2. Formalisation of 1. in first-order temporal logic

Temporal Monodic Clique-Guarded Negation Fragment (MGCNF)

Why?

Why MCGNF for Swarm Verification

2. Formalisation of 1. in first-order temporal logic

Temporal Monodic Clique-Guarded Negation Fragment (MGCNF)

Why?

- **Allow quantifications**
    - Universal $\rightarrow$ no need to specify size of swarm
    - Existential $\rightarrow$ no need to specify robot names

Why MCGNF for Swarm Verification

2. Formalisation of 1. in first-order temporal logic

Temporal Monodic Clique-Guarded Negation Fragment (MGCNF)

Why?

- **Allow quantifications**
  - Universal $\rightarrow$ no need to specify size of swarm
  - Existential $\rightarrow$ no need to specify robot names
- **Highly expressive**
  - Clique $\rightarrow$ each pair of nodes is connected
  - $\neg\exists\phi$ $\rightarrow$ relations that do not hold
  - Equality and inequality

Temporal Monodic Guarded Fragments

temporal monodic guarded fragment (MGF)

temporal monodic loosely guarded fragment (MLGF)

temporal monodic packed fragment (MPF)

temporal monodic guarded **quantification** fragments

Temporal Monodic Guarded Fragments

temporal monodic guarded fragment (MGF) | temporal monodic loosely guarded fragment (MLGF) | temporal monodic packed fragment (MPF)

temporal monodic guarded **quantification** fragments

temporal monodic unary negation fragment (MUNF) | temporal monodic guarded negation fragment (MGNF) | temporal monodic clique-guarded negation fragment (MCGNF)

temporal monodic guarded **negation** fragments

Temporal Monodic Guarded Fragments

temporal monodic guarded fragment (MGF)

temporal monodic loosely guarded fragment (MLGF)

temporal monodic packed fragment (MPF)

temporal monodic guarded quantification fragments

Decidable, 2EXP-complete [HWZ00,Hod02,Hod06]

temporal monodic unary negation fragment (MUNF)

temporal monodic guarded negation fragment (MGNF)

temporal monodic clique-guarded negation fragment (MCGNF)

temporal monodic guarded negation fragments

?

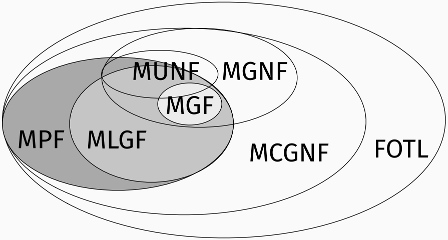
Temporal Monodic Guarded Fragments

temporal monodic guarded fragment (MGF) | **temporal monodic loosely guarded fragment (MLGF)** | **temporal monodic packed fragment (MPF)**

temporal monodic guarded quantification fragments

temporal monodic unary negation fragment (MUNF) | temporal monodic guarded negation fragment (MGNF) | temporal monodic clique-guarded negation fragment (MCGNF)

temporal monodic guarded negation fragments



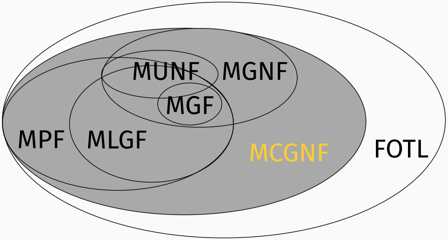
Temporal Monodic Guarded Fragments

temporal monodic guarded fragment (MGF) · temporal monodic loosely guarded fragment (MLGF) · temporal monodic packed fragment (MPF)

→ temporal monodic guarded quantification fragments

temporal monodic unary negation fragment (MUNF) · temporal monodic guarded negation fragment (MGNF) · temporal monodic clique-guarded negation fragment (MCGNF)

→ temporal monodic guarded negation fragments



MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg \phi(\overline{y}) \mid \mathcal{T} \phi$$

MCGNF

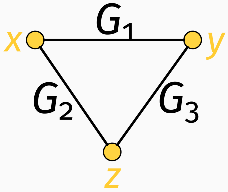
$$\phi ::= R(\bar{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\bar{x}, \bar{y}) \wedge \neg \phi(\bar{y}) \mid \mathcal{T} \phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg \exists u.\, A(x, y, z, u)$

MCGNF

$$\phi ::= R(\bar{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\bar{x}, \bar{y}) \wedge \neg \phi(\bar{y}) \mid \mathcal{T} \phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg \exists u.\, A(x, y, z, u)$



MCGNF

$$\phi ::= R(\bar{x}) \mid x \approx y \mid \exists\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\bar{x}, \bar{y}) \wedge \neg\phi(\bar{y}) \mid \mathcal{T}\phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg\exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg\exists u.\, A(x, y, z, u)$

MCGNF

$$\phi ::= R(\bar{x}) \mid x \approx y \mid \exists\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\bar{x}, \bar{y}) \wedge \neg\phi(\bar{y}) \mid \mathcal{T}\phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg\exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg\exists u.\, A(x, y, z, u)$

Equalities are allowed

MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg\phi(\overline{y}) \mid \mathcal{T}\phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg\exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg\exists u.\, A(x, y, z, u)$
3. $\exists x_1 \ldots x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$

MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg \phi(\overline{y}) \mid \mathcal{T} \phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg \exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg \exists u.\, A(x, y, z, u)$
3. $\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
4. $\neg \exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$

MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg \phi(\overline{y}) \mid \mathcal{T} \phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg \exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg \exists u.\, A(x, y, z, u)$
3. $\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
4. $\neg \exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
5. $\bigcirc \neg \exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$

MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg\phi(\overline{y}) \mid \mathcal{T}\phi$$

1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg\exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg\exists u.\, A(x, y, z, u)$
3. $\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
4. $\neg\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
5. $\bigcirc\neg\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
6. $\bigcirc\neg\exists x_1 ... x_4.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$

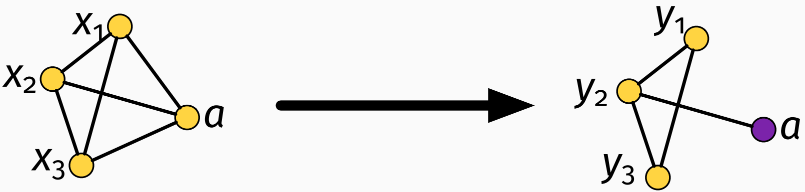
MCGNF

$$\phi ::= R(\overline{x}) \mid x \approx y \mid \exists \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathcal{G}(\overline{x}, \overline{y}) \wedge \neg \phi(\overline{y}) \mid \mathcal{T} \phi$$

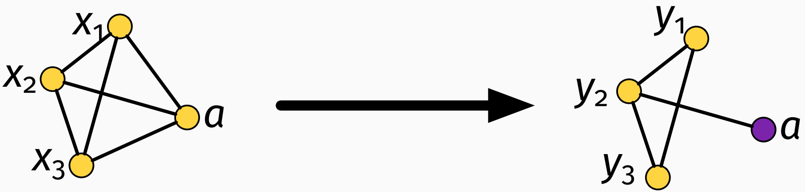
1. $G_1(x, y) \wedge G_2(x, z) \wedge G_3(y, z) \wedge \neg \exists u.\, A(x, y, z, u)$
2. $G_1(x, y) \wedge G_2(x, z) \wedge y \approx z \wedge \neg \exists u.\, A(x, y, z, u)$
3. $\exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
4. $\neg \exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
5. $\bigcirc \neg \exists x_1 ... x_5.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$
6. $\bigcirc \neg \exists x_1 ... x_4.\, B_1(x_1, x_2) \wedge B_2(x_2, x_3) \wedge B_3(x_3, x_4, x_5)$

Only in temporal monodic guarded negation fragments!

Use Case: Coherence

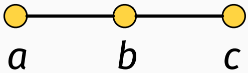


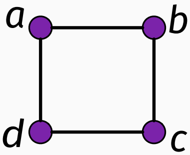
Use Case: Coherence



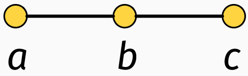
$$\exists x_{1\ldots3}(connect(x_1,x_2) \wedge connect(x_1,x_3) \wedge connect(x_1,a) \wedge connect(x_2,x_3) \wedge connect(x_2,a) \wedge connect(x_3,a)) \rightarrow \bigcirc\, \exists y_{1\ldots3}(connect(y_1,y_2) \wedge connect(y_1,y_3) \wedge connect(y_2,y_3) \wedge connect(a,y_2) \wedge \neg connect(a,y_1) \wedge \neg connect(a,y_3))$$

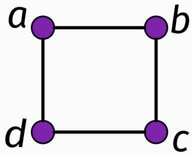
Use Case: Shape Formation





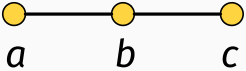
Use Case: Shape Formation

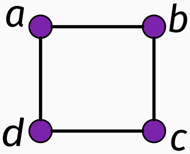




$$
\begin{aligned}
&adjacent(a, b) \wedge adjacent(b, c) \wedge \\
&\neg \exists x(adjacent(x, b) \wedge x \not\approx a \wedge x \not\approx c) \wedge \\
&\neg \exists x(adjacent(x, a) \wedge x \not\approx b) \wedge \\
&\neg \exists x(adjacent(x, c) \wedge x \not\approx b)
\end{aligned}
$$

Use Case: Shape Formation





$$adjacent(a,b) \wedge adjacent(b,c) \wedge$$
$$adjacent(c,d) \wedge adjacent(d,a) \wedge$$
$$\neg\exists x(adjacent(x,a) \wedge x \not\approx b \wedge x \not\approx d) \wedge$$
$$\neg\exists x(adjacent(x,b) \wedge x \not\approx a \wedge x \not\approx c) \wedge$$
$$\neg\exists x(adjacent(x,c) \wedge x \not\approx b \wedge x \not\approx d) \wedge$$
$$\neg\exists x(adjacent(x,d) \wedge x \not\approx a \wedge x \not\approx c)$$

Conclusions and Future Work

- MCGNF is potentially useful in swarm verification

Conclusions and Future Work

- MCGNF is potentially useful in swarm verification

- Verifying swarm coherence algorithms
- Avoid constants
- Investigating more use cases
- Practical decision procedures for MCGNF
    - First-order (temporal) theorem provers

Thank you. Questions?