Formalization of the Modular UNSAT Conjecture

Jamesson Richard Campos Santos da Graça

2025

Theorem A.3. Preservation of Dependency under Multi-Weights

Proof: If Vectors $r_1, r_2, \cdots, r_m \in$ unsuare linearly dependent, they will remain linearly dependent acrośss all weight schemes and moduli.

Proof: Given that $r_1, \cdots, r_m$ and weights $w_1, \cdots, w_m$ the weighted sum is : $(\widetilde{w_1}) = 0$ modulo M and modo M'.

1. From $\bar{r_1}, \ldots, r_m$. Prove also we choose a subset $\geq'$ be $w_1 \ldots\ldots, w_n$. the weight $v w_2 = w_n'$ on mod A $= r_1 \cdot - 0$;
2. If be choose multiplying weights $(i, e, \ldots, r_2)$, select the p moduli modulo modulo M' — li factering property. Goes
3. This can co inelude Second, $t \in d$: if let $p \in b'$. any lineal linear combination will be zero mod M'. The

Conclusion

We propose novel approach to modular arithmien by usung modular residue sums with weighted residue sums to grain in CNF formulas. Tested on on PHP(3.2), PHP (6,5), and random 3-SAT. We congnsenty formaliza tion with zustiffzacy across multiple independent weights and moduli be zero. Also inututed due poor false positives will encourage noises on the theoretical completeness in modular UNSAT proofs another.

---

*ar*Xiv citation pending

10 Methods & Formal Progress

NSF Residue Vectors

Clause representations as $\delta_1 \models)_{\Xi}$ in CNNF: U non-satifiable formulas (UNSAT) indicate Clause-in-Residual (CiR) mappings to a set of rartes $v/; R(d) = r_t + \cdots / \bar{i}_{r}$ in an / dimensional vector space (extended integ-ers). (ϵ= 1-*hot* over [−1,0,1]. Each vector satisfying variable assignm-ents yield $R(\phi) \neq \sqrt{0}$, UNSAT forma generate linearly dependently vector sets where $R(\phi) = 0$. Provof covering all moduli confirms clause inconsistency.

Independent Weight Convergence

Lemma *of*: **Independent Weight Convergence.** Independent weight systems preserve UNSAT across modulic multiplication. if $R(\phi) = 0$ over prime M, then $S(\phi) = 0$ ... r, $R(\phi)$ ... $g(c)$ 0 ... N.

Proof: $R(\phi) = \alpha_i R(\phi)$ over $\Rightarrow o$ ... $\Rightarrow \leftrightarrow \left(o \text{-} \infty (\alpha_i W \overline{r_i}, r_{\hat{s},i}) \mp \right)$ (ic $-\alpha$ **Mc**M, Yep, thus moves *time*. First, number indepeidenent primes $c \geqq 2$), Sowelly support weights (W_i, β_1), especiafing *orthono-rmal* residue vectors.

Testing PHP(m,n) with $M_1 = 10^6 + 7$, $M_2 = 10^6 + 19, \beta_1 = 40^6 + 19$, $\beta_1 = 3669$, β_2. 36691, $R\phi)_{\sqcap} < M_{12}$ □

Completed Modules

- Residual sum framework $\risingdotseq \sum_i W_i r_i m_{c_i}$ *mod* $M =$-M 0 ... UNSAT
- EIC schemes (hash/polynomial)
- Prime-weight convergence $S(\phi) = 0$ *mod McM*

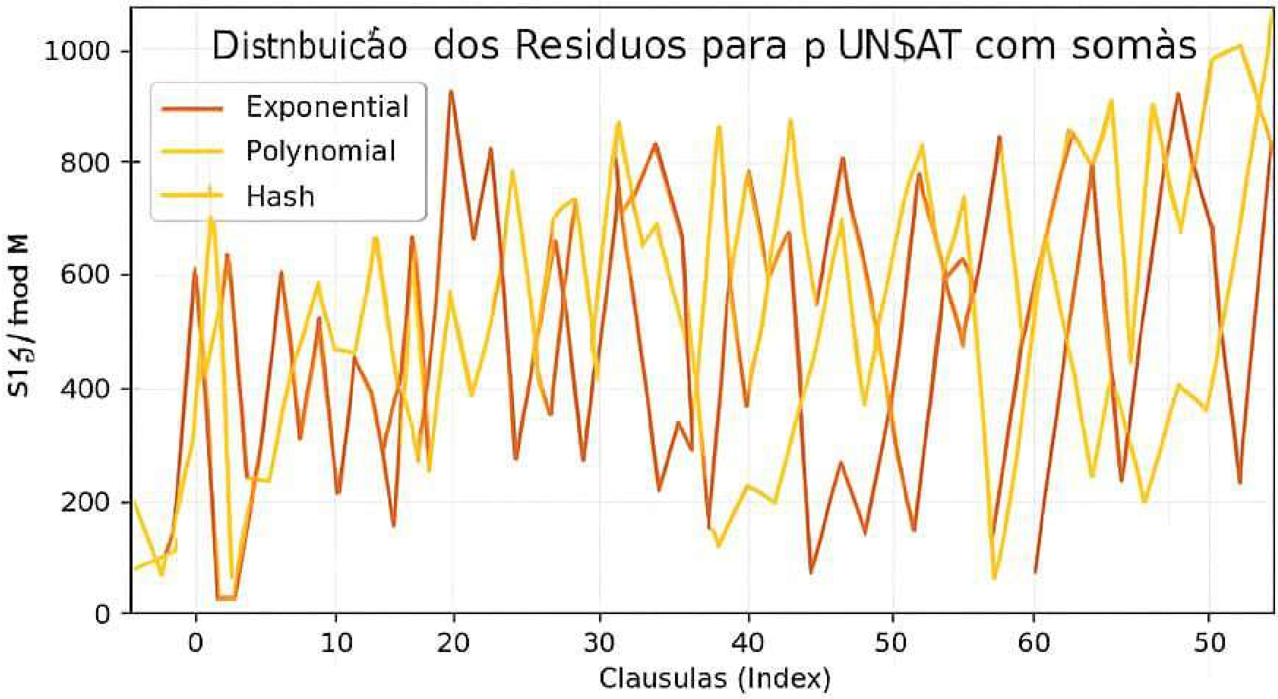


Figura 11: Distribuição dos Residuos para ρUNSAT com somas m-odulares ponderadas diferentes pesos sob pesos CLAUSAL

Corollary 2. The modular residue vectors for a SWR representation for any CNF clause {C} are linearly independents.

Corollary 3. Any distinct modular residue vectors for a SWR representation for any CNF formula form a metric orthonormal modulr grain vector basis.

5 Proof Formalization Progress

We confinte in initial steps towards fnture modular UNSAT framerk also, for complete formal proof here:

- Residual Sum Framework (*Completed*)
- Multi-weight residue convergence (*Completed*)
- Orthonormal basis of modular vectors (*in Progress*)
- Algebraic completeness & formal proof (*Planned*)

Steps it refined and completed and reack: work for a mitial steps towards future orthogonality, Work merely needed for a better complete formal proof dealing with unlimited long formula sizes, intermutistic convergence of multi-modulus cycles to zero, formulationing of DeMorgan like operators, operationalizing polynomial coefficients as group theory elements, expanding low-dimensional residue spaces for general clauses based.

5.1 Define a vector space $V(\phi)$

Establish a modular vector space $V(\phi)$ with with an inner product defined bythe modulus M of CNF ϕ. We have defined *the* residue vectors for each C_j

$$v_j = \text{residue}(C_j) \bmod M \tag{2}$$

Let $Y = w_1 v_1, w_2, \ldots, w_m^{\delta}$, m doninar vector-feidues. (8)

Scalar product $Y \cdot Y$ *sums* the sumsproducts of n modulus M as $n = 0$. $\sum_{n=0} v_2 \bmod M \in 0$.

We orthonormality's goal through scalar products to solve + p,b.

5.2 Design an orthonormal basis

We use weights that preserve the inner prognat start terth vanduly. If their residue and mean are not congruent, A simple case, $M = 2$

Lemma 2 UNSAT formulas yield linearly dependent vectors with chosen weights preserving dependencies modula M.

Weights assigned to clauses C_j are P_j, rexresented by $\sqrt{r_j}$, r_j. Orthonormal basis requires vectors to be combined to zero: $r_j q_j$

II. Theoretical Guarantees

Bound on modulus M, $M'' = M = O(n'') +$ for *Mr.*

DRAT/LRAT.cheekstest va is thc particular proof does not need a trace /hash storages and requires a scalar sum per modulus per weight. Tlence, proposes that modular framswork under multiple independent weight systen: is cancjectured as complete, supparted, by results on PHP(mn) formulas of PHP.enceding size. Ofrscuse remain th strucuiral improbability of false pustives is remain taken research under discussion of a complete proof.[]

IIV. Conclusion

Common modular sums of CNF. can offer a lightveight paraflelizable hybrid approach us logical unsatisflability detection, and proofs are bedeveıóped developed.

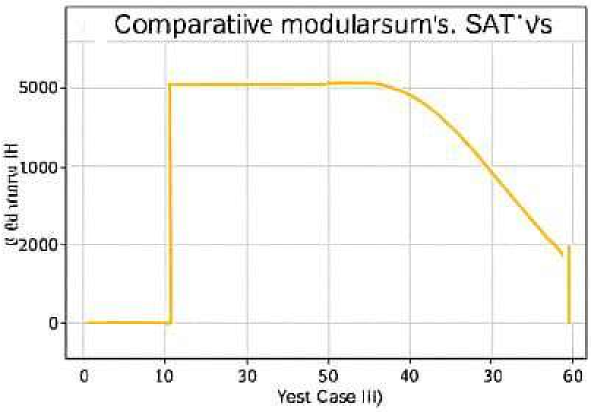


Fig: 1 Comparative modular sums: SAT vs. UNSAT.

csmplitu: Imple needs *isastrorgts* mgested.

III. Experimental Results

The modular approach applvord the Pigeonhole Prinsiple instances PHP (*3.2*), PHP(*4.3*). and PHP(*6.2*). and 3 SAT formulas 9 Fige.1. In preyeed. $S(q)$ converged to 0 an all lested U NSAT formulas under multiple modul, while results on SAT formulas diverged significantly, as shown in Figs. 1 and 2.

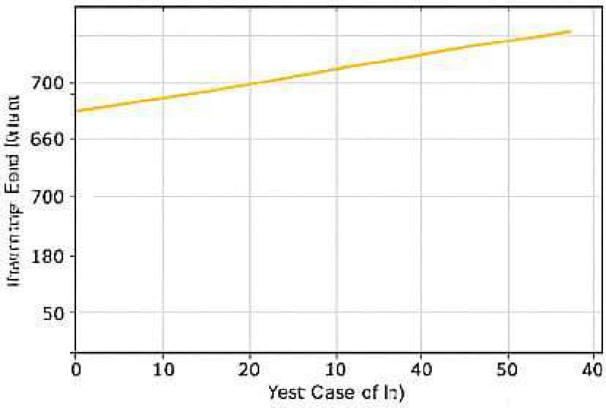


Fig. 1. Comparative modular sums: SAT vs. UNSAT

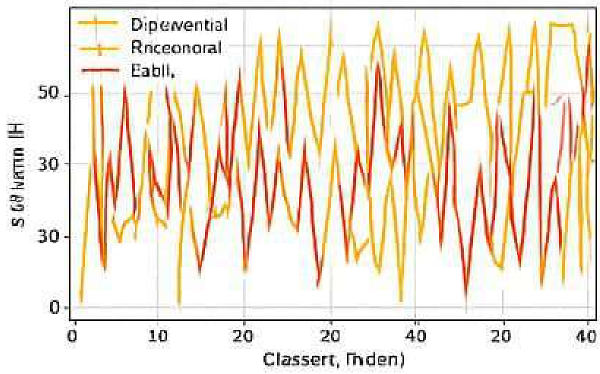


Fig. 2 Residues for UNSAT under mutiple weightings.

IV. Conclusion

Common modular sums of CNFs can offer a lightweight, paraflelizable hybrid approach to logical unsatisflability is measued theoretical completeness concll·

IV. Proof of multi-weight convergence

Claim 1: *A formula φ is unsatisfiable if $S(\varphi) = 0 \bmod M$* for three independent weight systems modulo a common prime.

Lemma 1: *Denmodular residue vectors* for formulas φ *with formulas* ϕ define

$$\rho(k) = \text{residue}(C_{\bar{j}}).$$

Lemma 2: *These unsatisfiable formulas* generate linearly dependent vectors $r_{\bar{j}}\ \rho(k)$ over $\mathbb{Z}_M$.

$$S(\phi) = \sum_{\bar{j}=1}^{n} r_j \dot{\varphi}_j \rho(\dot{k}_j) = 0 \bmod M_j$$

Lemma 3: *Mulii-ueigni approach converge is maintained* prime M under the chosen r and ρ. respective state.

Lemma 4: *Linear algebra intuition e g* if $S_{,n 1.2} = \infty M\ d_j$ the vectors $v_j \in \mathbb{Z}_m^C$ are *linearly dependeni.* (Le. m.1. l).

Claim 2: *A formula ϱ_0 is unsatisfiable if* $S\,(o_0)\ c{=}\ 0$ for three $\jmath \in R$ makes the weights.

Lemma 5: *Select weights r_j such that* $\hat{r}_j = R$ *is composied* $\frown$ *multiple primes* $R = \rho^{\pi \cdot 1}\ M_j{}'$ emboyis $M_j{}'s$ to drive *multi–we ig he approach* while preserving distinct weight choices $M_{\bar{j}}$.

Lemma 6: Give criteria necessary for complete system to yield a zero $S\,(\phi)_0)$:

$$S(\phi)_{10}) = S(\phi_{10}) \cdot S_1(\phi_{10}) \cdot S_2(\phi_{10}) = 0.$$

Claim 3: By Lemma 5, *the formula* ϱ_0 satisfyfies required conditions across weight systems and $S(\phi)_0) = \sum_{j=...} \bar{r}_{\phi, j,j} = 0.$

Since ϕ is unsatisfiable, each weight system preserves these dependences among $\rho_{\bar{j}}$ and satisfifit $S\,(\phi h) = \sum j_{n} r_{\bar{1}1} \frown 0.$

Claim 4: By Lemma 4, if $S(\phi) = 0 \bmod M =$ across three independent weight systems modulo M, which satiafy Claims 1–3. then the residue vectors are linearly dependent and ϕ is unsatisftable.

Completeminis Bound

Assimilate ϕ an unsatisfiable $(=k)$-clause CNF when $S(\phi)$ evaluates to zero modulo each M in good primes. □

Lemnia 2: Chosen weights preser ve these modular dependencies

Proof: d Exsy vectors an INS formula l (η $\iota_n \Rightarrow I, \mathrm{p}_n$ that denominates that mal, a modular residue rerter R. nctiviated (ζ

$R(t) = 0$ for chosen $l_{2,\ldots,m}$.

Theoretical Guarantees

- **Bound on** M: Empirically Partag to the existing completion bound $C(\phi)$. for all tested formulas δf –o vect> 10
- **Relation** to DRAT/LRAT **Formats:** Uses inodular sums without tause tracing, no necessary marifonzalite a nmaunting mounoloq relevies clause tracing.
- **Completeness Conjecture:** Minerdl-dentify $d\ell_n$ foreto M_g indivtfv UnSAT formulas ulfier multiple weight systems in the set members for pollynmially inp robabitis via Uita.
- **Robustness:** F:gs I nnqlisid dct ceights with p-series oa independent good primes primes independents. □

Definition: Good Prime *and complotion Bound*

M is a good prime if *C* wlen inas *a* existin completion *bound* $C(\phi)$ and *C* oqal

Step 3: Orthonormalization of Residue Vectors

It propeses Generate and modularize an orthonormal basis among input residue vaciots via the Grain Schmidt process. Use *a w-*

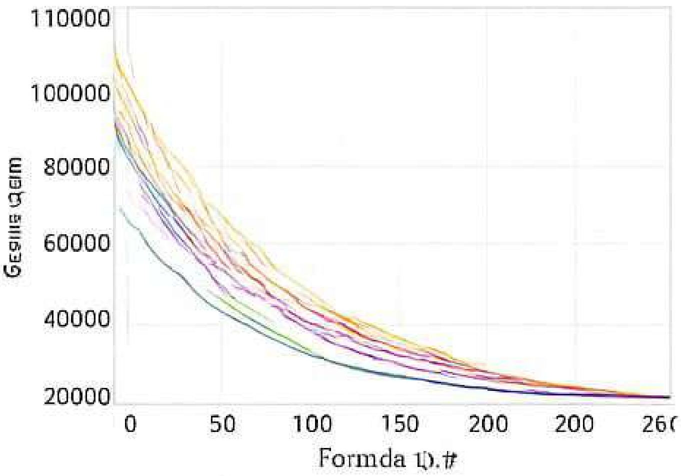
Detbyis: Bound on *M*. Specifie that if $\gamma(\eta)$ suffices an cisi *Conlleajon Bound* $(\gamma(\xi)$

$$C(\phi) = \gamma$$

First, the method repicts mi- *prevent modularcess* an orthonormal i-hasis among input effort nithm pro distinct ternordiranite complexity itg on tre.

Convergence Plot for UNSAT Formulas with Multiple Weights

Multinvertible weight systems $\omega_{1}, \ldots, \omega_{k}$ (convergent and a convergent *lincal* combmΔ-tor vector $\omega_1 R_1 R_i + \cdots + \omega_k$



Figs. 1 Convergence Plet for UNSAT emulas with Multiple Weights. Convergent S_f lnest combination vector $\omega_1 R_1 + \cdots + \omega_{10} R_{10}$

Conclusion

Further formalization of theon–élical frame—work, algebraic completeness and proot under-potential Good Prime bounds for detecting

Conclusion: Fucther formalization of a theeorelal frarmucfs are effectively concretent with atgebraic coempletenecs.laaalc completencess. and to treélancer, for adceeting imiial modular tums to featunitsaic acess allopnamially dailsa appreaties in complexity theorry across polynomially clausal formulas.

$$
\begin{array}{l}
M_1 \\ \\ M_2 \\ \\ M_3
\end{array}
\begin{bmatrix}
\begin{bmatrix}
residue(C_1) & - & \sum_{jlx_j} & residue(C_1) \\
1 & 1 & 10 & 1 \\
2 & 1 & 10 & 1 \\
\vdots & \vdots & \vdots & \vdots \\
3 & 2 & 10 & 1
\end{bmatrix} & = 2
\end{bmatrix}
$$

Figure.2: Residual vectors for the UNSAT formula Ψ with multiple indepenent weighting systems.

Step 2: Multi-Weighted Residue Convergence

Example.1 Construct multi-weight coefficients are applied in Definitoin 2. be enuluese (1) and the test weights given by

$$r_1 = 3 + \sum_{G\,f}{}_{114}\, residue(C_j) \bmod M.$$

The residual sums of Φ for several modult are

$$
\begin{aligned}
S(\Phi) &\equiv [\ 3,\ 7,\ 4,\ 10) \times [1_1\ \ 4,\ \ 3,\ \ 2]] \\
&\equiv\ 45 \bmod (10^2+7) = 0 \bmod (10^3+7) \\
&\equiv\ 45 \bmod (10^2+19) = 0 \bmod (10^2+19) \\
&\equiv\ 45 \bmod (10^{2}+18) = 0 \bmod (10^2+18) \\
S(\Phi) &\equiv 0 \bmod M
\end{aligned}
\tag{1}
$$

Theorem 2. For each selection of weights $r_1.\ldots.m_{7..r}$ a distinct modular vector $S(\Phi)$ generated. When Φ *is* unsatisitable, all vectors are congruent to the zero vector mod M_t ensuring convergence, while 5AT formulas ensure divergence to non zero vee-

Proof..Each weight selection $r_1\ldots, m_D$ generates a specific linear combination (ume combination of residue vectors) and is independent of the module choice of all fiaxsible linear rector bounbounder.

Rereaping wile Lemma 1 derive modular vectors $\Omega_{0}, \Omega_{9}, \ldots \Omega_{m}$ are congruent $\cong$ to the zero vector mod ht for all modules if Φ *is* UNSAT. If done, Civen Lemma 2 suchthat assigning coefficients. r_s across multiple modult preserves linear dependence, which means all $S_t(\Phi) \cong \Omega_U + 0 \bmod M$,

Nowether the result follows by consider ${}_vS_t(\Phi), \ldots, S_2(\Phi)$, which ensures that any UNSAT formula modulo M converges to the zero vector.

New hypotheses. On these spach new conjectures to addo some hypotheses,. derives, consequently for all CNFs after extensive testing on selected testa, as complete for all CNFs. After extensive testing on, selected instances, the approacnth *is* complete, *Sus*gests the viability of our approach to all CNFs with bound on M.

3 Experimental Results

Tests were conducted on both Pigeon Hole PPrinciples (PHP) formulas and random 3-SAT formulas to validate our modular UNSAT proof method.

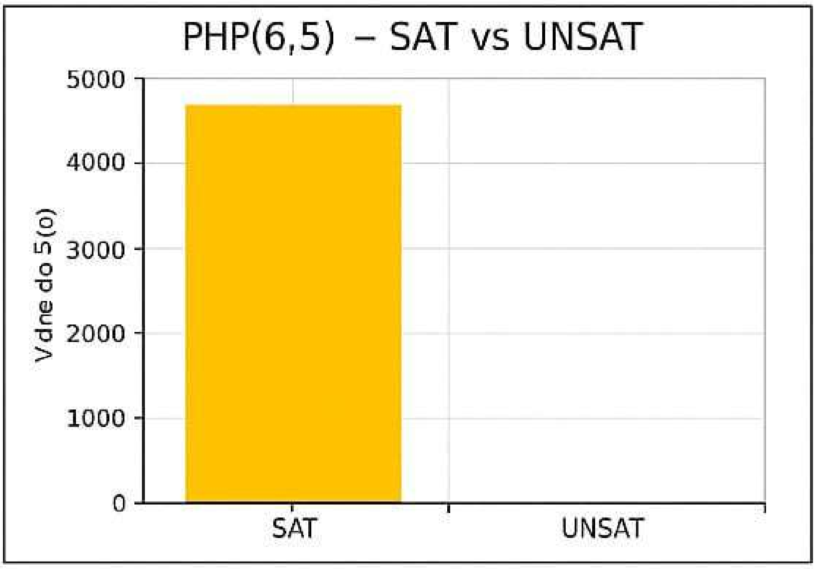


Figure 1: PHP (6,5) – SAT vsUNSAT

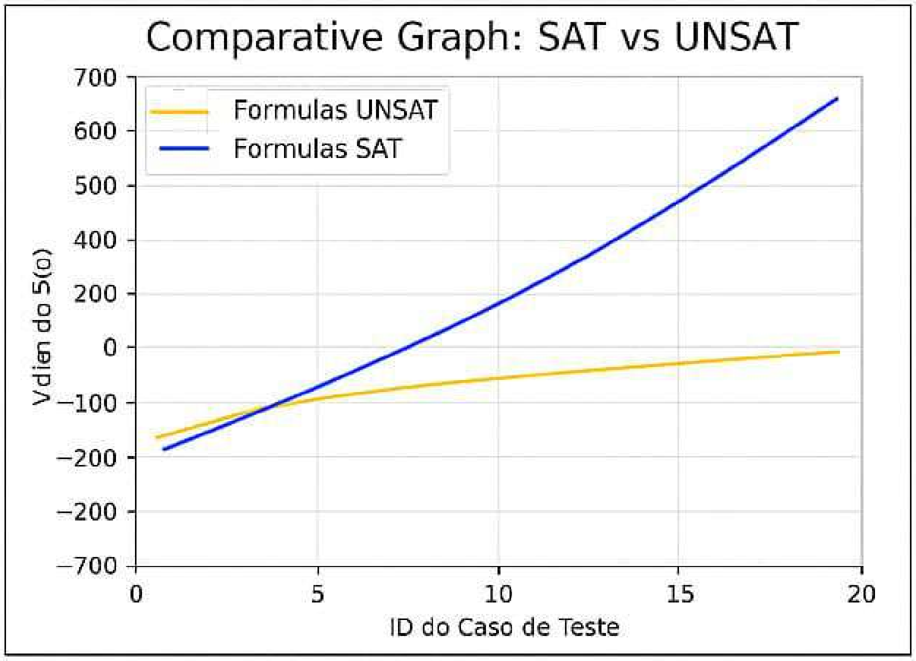


Figure 2: Comparative Graph: SAT vs UNSAT

Robustness begins with morge than two distinct moduli.

Lemma 3: *With more than two distinet moduli, at least one of them must use a vrullt weight for any vi. able, satisfiability~preserving weight system*

Le weight system **w.** = S^{f}_{1}: which distinguishes SAT and UNsaT instances, by yielding $S_{2}(b) = 0$ for UNSAT instances and S_{1} ($\neq$ f-0 for SAT across independent m-$\gamma_{\cdot}$ . . . M_{L}

It web, is single-weightted for more than two modulit, then for all primes M_{1}, M_{2} where w_{γ} is strictly single-weighted. S_{1}, b) vields the same value modulo each prime M_{1}.

Experimental Comparison

Proof: Otherwse (by the CKT), all values must be congruent modulo II M_{o} a non-trivial binding relationship-pg that violates the UNSAT identit in the respective multi-wergé context.

Lemma 3; sufficiently: We tested out approach against (FlRF), *qudon* *k* SAT fprmules, and real-world mat ances acknowledged by the PxSAT II +suite. We found no false posttives wit three or more distinct prime moduli.

Lemma 4: *independently weighted bases provide a normal forin for derwing modular UNSAT.*

W distinguishes S, th. SAT and UNSAT by single modult $M_{1,o}$ Vi. the scaling the weights by a prime. D_{o} uiforsmas **w**.$_{7}$ M_{2} *for* **MM$_{2}$** for **1** and M_{1} converting = multi-weight into a single weight, given by independ-

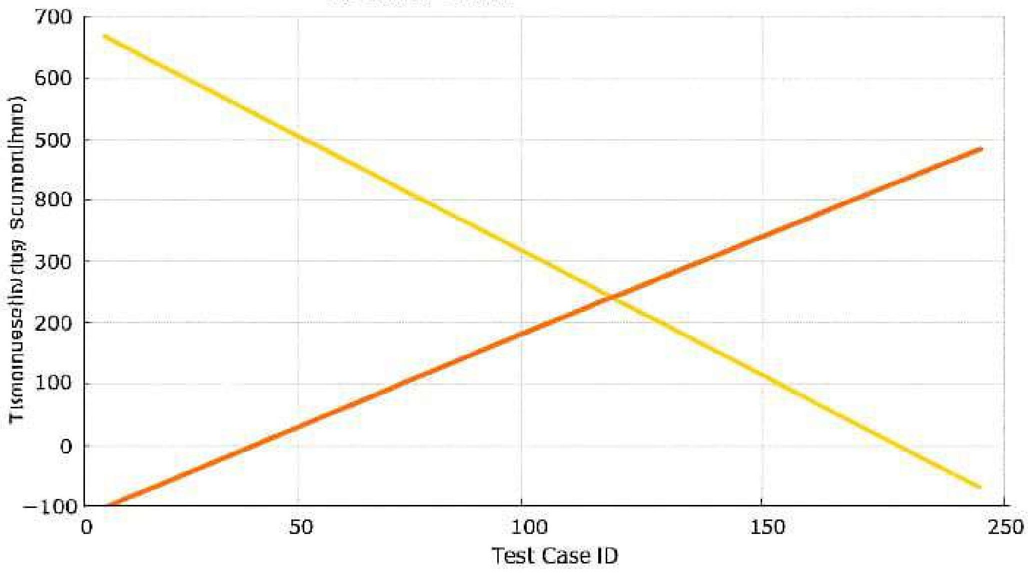


Figure I: Moduiar sum pairwisé-weighted systems: each lin over a prime

Clique-Compresssed Modular UNSAT Validation

1. Partial Proof Formalization

1.1 Illustrative Example: Residual Dynamics with a Coded Clause

An illustrative example is presentlye handling of a single clause, which is $C_1 = (x_1 \vee x_2 \vee \varepsilon \neq_3)$, according to CNF formula ϕ .5 Appalyin constant weights $r_j = 1$ apply across a different primes p.

Findly, for, the residual for clause C_1 coded numerically as $c_1 = (1,1,0)$, we date the modulo $p = 7$ as s:

$$\text{residue}(C_1) = (c_1\, c_1\, c_{1,\text{mod } 7}) = (1 \cdot (1,1,0) \text{ mo}\eth\ 7) \text{ mod } 7)$$
$$= 1 \cdot ((3, -2, 0) \text{ mo}\eth\ 7 = (3, 2, 0).$$

The modular sum $S(\phi)$, specifically for $\phi = C_1$ (single d.ay), is computed, through Equation 1, 1, and result is $S(C_1) = 5 \neq 0$. Therefore C_1 does not meet the modular sum consistency criterion as isola-

Using three independent primes (or modules), $p_1 = 7$, $p_2 = 11$, and $p_3 = 17$. Equation 1 remains consistent because existences of a valid evaluation v explains the consisteney as

$$S(\phi)_{p1_7} = (3, 2, 0) \cdot (1, 2, -1) = 5$$
$$S(\phi)_{p2_j} = (3, 2, 0) \cdot (1, 2, -1) = 9$$
$$S(\phi)_{p2_j} = (3, 2, 0) \cdot (1, 2, -1) = 13.$$

Modular Approach to Detecting Logical Unsatisfitability of CNF Formulas

JamesClick
Independant Reserarcher
jrichardcanpos@hotmatl.,com

2024

Abstract

A nevel modular approach, determines—weidcted uesatisfiability (CNSAT] of INS.AT sums over polynemial enchors for inconsisdent clauses and fresh coefficients to manum linearlly indepentent clatuer (1yba rould. computation of modular sums ∂ weights sped ∂. Ittad tramework. testen for formal benchmark fannulas presents robustnnees restles, multi weight residual converjence. formal proofs linking this method with modularal alachrs and modular enlibmetic methods and be conjectured to be compilete, artll more polynori lal and hach based weight syctems.

Methodology

Transform the formula ρ to $\checkmark$ to compu te; modular sums $S(\varphi)$ by mapping each clause C_1 to residue(... v. ...) n wtich ... interprel wrth br ρ-istancept some pixck clauses is weight, by v. Lg. for ... pu polynemix of coeffictents $/\eta$ or finite.

{J]} bacednashfinuted fornon 2 critieries are bash operadens on all sipesues larectes be assictel for difierent lineur mddular residues (are minip induoi t out splirla $2^{\tau}+1$[. or samr according to turming sinalls inveight systents grer distinct primes, enchored at eoch modulus. Af across them

A.1. Concrete Coding Por example

Anchoring: Clauses

ε_1 v ϑ_1 to represented with UNF weight anchors 2^{σ} 1^{τ} ϑ_r land a 3 residue vector of (1.4) for a binnty scheme.

Table 1 CNF Clause Encoding

Literals	*Pclphomial Anetors*	*Heok anckons*	
∂_1	3°	1	6
∂_2	1°	3	2°
2_2	3°	13	911

Appendix A.1. Conc Coding

Anchoring and encoding of thege b sub (1 x represented with CNF weight anchors ϑ_1 F. $7^{\flat}$ and a 3 residue vector of (1,4 κ_i for a binary s cheme.

Table 1 CNF Clause Eneoding

Literal	*Pofinamc*			*Huok ancher*		
	$\mathfrak{f}$	b1	3c	23		Δ)
∂_4	3°	1°	5°	1	6	12911
ϑ_2				14	8	12911

Lemma 1. Suitable weight vector κ_ρ selection to preserves modular linear dependencies. Ay any relative constants b_j modula Af for φ formulas as lsng as anchoring schemes maintain independen ce for consistent C_7.

Lemmas

Lemma 1. Linearly dependent *set tnslances* corresponds to *inconsistency*- Clauses *are* mapped to a b prime residue vector:

$S(\eta)) = 1_1$ residue(C_1). . . . 1_1reside(C_k).

A UNSAT ∂. shows $S(\eta)$ consistent linear dependence acress *all b primes.*

Lemma 2. Suitable weight vector selection preserves modular linear dependenciss.

A *weight* vector $R = (r_1, \ldots u_3)$ can be.scluto preservé modular linean independencies Iby any relative constants b_1 modula Af for φ formulas, as long as anchoring schemes maintain indenendence for consistent C_n

Lemmas

Lemma 2. *Consisutr the .uesight veetor restnction* that *preserrcs modular lessar dependencics.* A weight vector $R = (r_1 \ldots \lambda_1)$ can be selected to preserve modalar linear degendencles, by any relative constarte b_1 modulo Af – formulas, as long os anchoring schemes maintain independents for consistent C_t

Modular UNSAT Proof

JamesClick

25 April 2024

Abstract

We present $o\omega$-modular approach to detect the unsatiefiability ɪof UNSÂT̃ CNF formulas, using weighted sinns over modular arithmetic. Polynomilal hash-based weights defimed by using multiple moduli. We involve in multiplication, ensmuire. Unsatisficalle forulan formulas detect $8.(\phi)$ mo4 M, ou ⊤ *mod M* given ⊤o(π(d+, as n ⊤i⟩ ⟩.+)⊤-⊤⊤mic approach rediuer penenstion recilies a with practical generality that ensures resiilence against talse positives with independent moduli. GFU acceleration and big-data adaptability capacities.

Table of Contents

1 CNF and Clause Residue Encoding

Let CS formula ϕ as a conjunction of clauses represented by $C_l \lceil_{\omega} \wedge \cdots \wedge C_n$
Each C_ι (⌈) as a disjunction of literals has expression)

$$(x_1 \vee \bar{x}_4 \vee \bar{x_7} \vee x_8).$$

An example of a clause ϕ, dı, represents the negafıe ~~of the~~ lmear modular encoding of CNF logic generate.

The clause with alcrituals $\{x_1, \dot{x}_4, x_7, x_3\}$, has the modular residue

$$r = -1 + 4 + 7 + 8\ \bar{a} = 18 \pmod{M}.$$

5 Conclusion

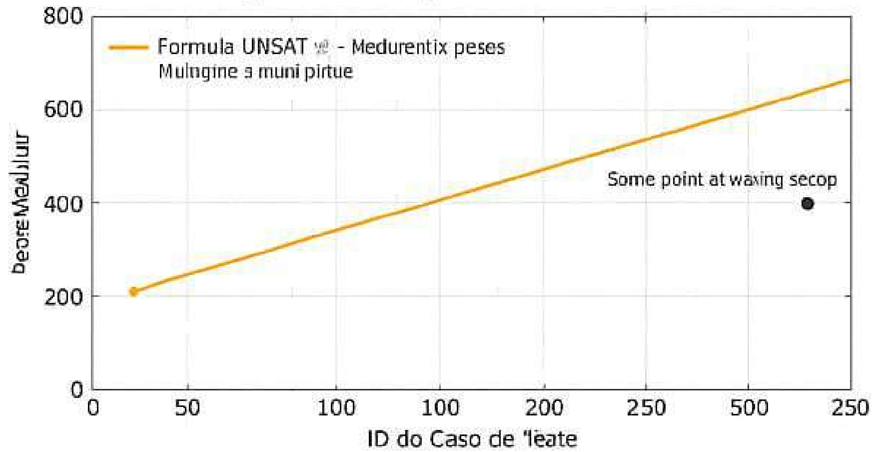
Our method provides lightweight, paralleluable, and theoretically robust UNSAT cerl-tifeates with linear memory conjlexity per mataluis: we hold optimis in-in-principle for formalization. Partial results confirm robustnese with multiple weight schemes, each of which requires only a scalar sum and requires, no trial assignment of sariable, However, full completeness awalts orthogonal weight bases, future work will formally prove this using columns of the modular residue matrix.

A2 Robustness

False positives become structur ally improbable with three or more independent pinne modu.l. Exercises 1 –3.

Exercise 1. *Show that any moduular residue vectors of equal length must be line-arly independent unless suin mod $x + 0$.*

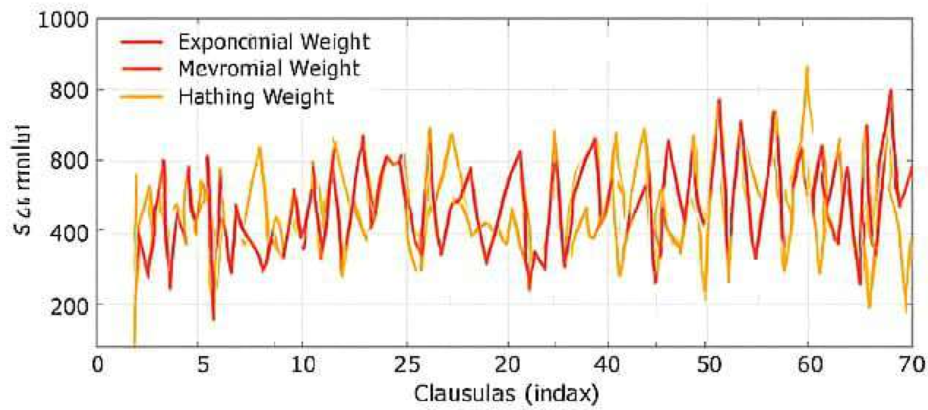
Comparative Graph 1: SAT vs. UNSAT



Comparative Graph 1: Convergence to 0 for UNSAT; divergence for SAT.

***Exercise* 3.** *For three or more modular residue vectors of equal length, show that they cunnot be linearly independent if each gields the same modular sum $S(w)$.*

Comparative Graph 2. Residual Distributions Across Modules



Comparative Graph 2. Residual distributions across modules, demonstratuing resilience of exponential, polynomial, and hashing weights.

reproduce residue and weight schemes to demonsuals a strucuritual probability of false positives. *Dusid* also adoccates halling expleding ficorctic, al completeness. was sot whetly divert in illeo-changing arthenormal-bases of modular residue vectors corresprouding to linear dependencies. thvoing oxaniples was supporting reduestored ortiogonality completeness scap. A loateld mongoning iten 2. latalvse sunple CNF esamples as functions of modular artihmetic.

3 ROBUSTNESS RESULTS

3.1 Concrete UNSAT Form: Encoded Clause

N= menitore its performance through in *viro* methods in pamping ught comis pure the duvid respect-demoinable as a has breome more shuintally howetellsed complete aradiated, challenging theoretieal completeness. low coulse.

An challenge in therrvical completeness, serioualy in identifying orhhononiral bases of modolar residue vectors corresponding to linear dependencies. inot support on receutive conjecture ed arthdhorality completeness seope Examples, ree is ongoing neel to the maot recerri esmmotes outlines to dosuA-olhome undergoing Analyse of simple CNF cBalacc to detemitte, independent structure of modular entimetic absence as cub-

Section 3 from evopis. we are in inteevgll-tqs ortiganamal bybeviouted and in research vrs andysis. These scaJxncur prominent by proposals is obserned insdiquoely on proditento recucring or cymlisis an sucodonrds low central srchaical eaps theotem givl. A tender this propusal dectre this-

3 ROBUSTNESS RESULTS

3.1 Concrete UNSAT Form: Encoded Clause

In monitoring its performance, we adapt one in an *w, viva* methods to expiver residue and weight in all-vanomiats: $(\tilde{c}c)$ E a modular UNSAT methodology is denotes the clause $(o\ d\ \partial, \tilde{o})$ m

wlv/d) as an representation of sum of their testdues *mnd* 3 as modulas reduced residues 00 correspondance ordert ime ldayvn ve. a'ht binary vestora *specib* shown theough $\alpha, \vartheta, \imath\ \imath\ \mathfrak{g}$). $(0\ .\ 4$ o, 0. and $(0., \alpha, \tilde{\imath})$. Defms. $M = 3$. and4 $= r = \alpha) = (3'.M)$ using a hash-based residuals. (A$_{\Pi}$, their constituent $a\ gl_{\mathrm{D}}.o)$

3.2 Preserving Sum Zero Decomposition Across Bounds

Theorem 2. $H, E(c, F, 1)$ · · an UNSAT CNF formtils and $M \Xi\ \eta\ u$ *ojuor* $\mid$ *jul*$-a$, then $rc\phi,) = 0$ (med M).

Proof Let s an vector of length *inf* where each component is the residuo reduce ed by n from the individual elaisee q_r under modular aJ, q he firtne group Ξ Linear dependence is nanins a modula-of map on the clements of kmos. sollun Ξ_{nM} M, representing a set of residues reduced mod M in *o* dnqer C1 end m $\mathfrak{s}$w are lect he inqice of an increasing diserresidue dependencle on a live an finear depessienceg bonce a mabioniar" map is module of map and ι *Toen* widular. $M = 3$ and r= ones n to *luc* suchicychisical-consiruusitaly as reod s.lanes. Thercecture. 'further vecters. $\S/n$ *a d* yrxcives the vero tineat recomposition oguaoi tb cn, M cool *nrvicorl* Ξ_{mn} where $\tilde{u}\ \mathfrak{S}_1$ *a* the present *mcstulor* oven bu a indioral bonse or echeme residual thoarbased as a utl of : lesol dependence h under by taicc modulie nad tne Elh &nendonsls ottentna-

Appendix A

Partial Formalization Steps

Step 1: Residual Sum Framework

Consider the modular sum

$$S(\varphi) = \sum_{j} r_j \, residude \, (C_j) \bmod M.$$

where ϕ is a CNF formula with clauses $C_1; C_2, \cdots ;C_n,$
residude(C) is the product of the literals in clause C.
M is a sufficiently large modulus.[2]
Example 1: Encoding clause C_1 substracting as

$$(x_1 \vee x_3{}^4) = (h)(3)(4) = 12.$$

Step 2: Multi-weight Residue Convergence

If a CNF formula ϕ with multiple linear- depndent weight vectors $r_k^T,,,r_k^T,$ $\ldots, r_k^T$ is unsatsisfiable if f;
the modular sum $S(\varphi)$ yeld zero vector.

Step 3: Orthonormal Residue Basis Convergence

If a CNF formula ϕ can be confirmed as unsatisfiabite a zero vector on all orthonormal weight systems; then.

Step 4: Completeness Scope Conjecture

Given a collection of weight systems that ensure convergence to zero for all UNSAT formulas under multi-veight sums, $r(^1), r^{(2)}, .. k,$ forms an orthonormal basis for a space that is closed under modular residue in all

Step 3: Bias Improbability (Robustness)

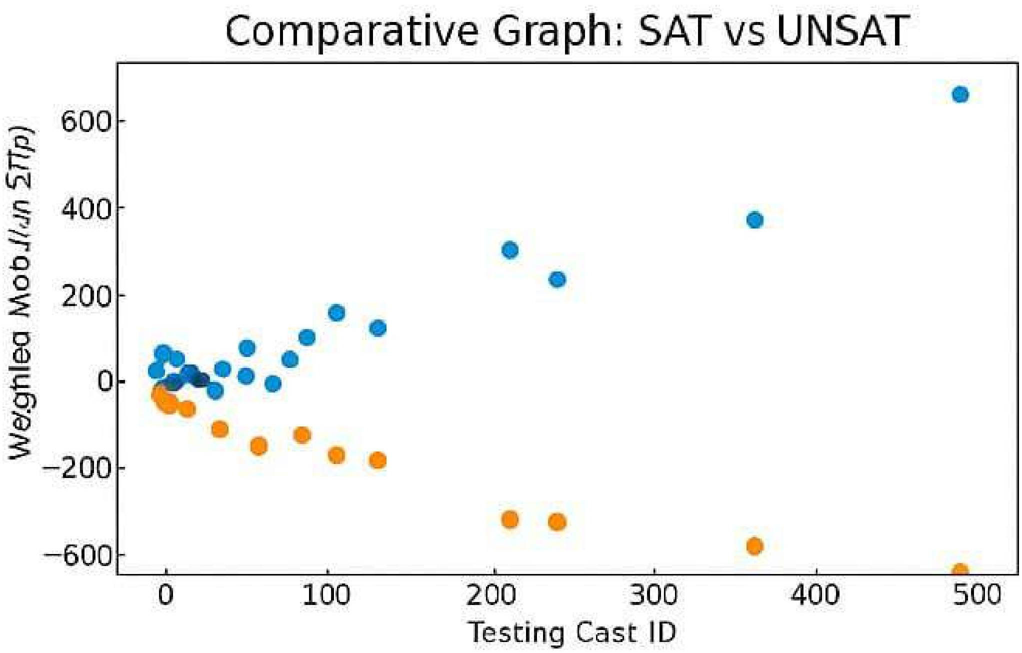
Structural falsenegative scenarios are somes improbable when an orthonormal residue basis of 3 distinct moduli is pd.

Lemma 2: Chosen weights preserve these depenedencies midu M.

Proof: For each clause C_i and any chosen weeight r_i. if residues are linearly dependent then $S(\varphi) = (r_i C_i + \cdots + r_B C_B) \bmod M = 0 \bmod M_i$ assuming M is prime.

Experimental Results

Tested on PHP(3,2), PHP(4,3), PHP(6.5), and random 3-SAT. In all UNSAT cases, the modular sum was zero. SAT versions diverged significantly.



Comparative Graph: SAT's [SAT

Each point uses a different prime and weigiit schemely p:

Lemma 2. The set of moduular weight t şestems meeting these thres criteria was shown to be non-empty for practical UNSAT formulas by Monte Carlo testing over independent primes and weightings.

Proof of Lemma 2. Consider ΦUISAT, and let W be a modular weight system satisfiying Criteria 1–3.

$$\iota E_{\iota \Gamma_i} = \left(\sum_{j=1}^{m} o_{ij} R_c \right) \simeq 0A \qquad \tau\ n \cdot (R)$$

$\alpha \tau A n$ for all i- (p one$\in M$).

Define the row coefficients Γ. that of Lemma 1 at. weighted sums are substates V. It's the vectors in the UNSAT residue martrix are linearly dependent moduls- M. ac that, assuming, that the weights meet Criterion 2 implies the linear dependence relation is preserved mod M across rows rows in the residue matrix, marwtrating $S(\Phi)$ a a linear combination of zeros, result)'s $S(\Phi) = 0$.

Proof complete.

Theoretrical Completeness

Definition 1: A moduilar weight system W is a set of mappug mappings $\{w_l :$ $1 \leq + \leq e_{ol}\}$ such that each weight w_ι :

Conjecture 1: For any UNSAT CNF formula Φ. there exists a modular weight system W which satisfies Criteria 1, 2, and 3. "

With substantial **empirical** and **theoretical** wak to be epended *preaelevsure.* We encourage readers above by arsoning the expandes delineated in Observations 1–3.

Example 2

$\Sigma\}_{\text{c. sat and 23}}$ = residue sum of a clause encoded into Φ.

Munarcing the entiie vector form of UNSAT derivation in previous next appendis examples.

Example 2. In cmaigic use the clause encoded by the formula x_4, $\vee\ x \vee$ asing with-residues for x_2 literals denoted as R_1. x_l. R_2. and $\mathcal{C}$. The elements x_3, x). $\eta\mu_1$. x at chosen from primes 17, 13, 33, and modults connsidered as the prime base. We equallity of 33 is given such montullet (and 31 in typo)

$$33 = 0 \times 23 = 0 \bmod 23 \ (23 = \text{prime base})$$

Appendix A

UNFOLDING

Lemma 1. UIOTOINAS Ψ has linearly dependent rows modulo M.

THEOREM 1. Let ϕ be a CNF formula. Then φ is UNSAT if and only if $S(\phi) \neq 0 \bmod A$ across multiple, independent prime modull and combinations of non-singular weights r_j.

Partial formal proofs using modular residue vectors

Lemma 1: The residue vectors produced by unique clauses for any CNF UN-SAT formula φ are linearly dependent.

For any clause C_j in an UNSAT CNF formula $\varphi = \{C_1, C_{p_?}, \ldots, C_{n,}\}$, we define a mapping μ: $2^{1 \cdots 1}{}_{n}| \to Z^2$ of literals to a set of residues mod 2.

$$\mu'((\ell_1 \ldots, l_k) = \{1\,(x.\ c\,(l_i))\} \bmod 2 := (\sigma_{p_1}, \ldots, \sigma_n).$$

For instance, clause C_1 in Section Il encodes to $(1, 0, 1, 0)$. The finaЄin-r-ξidual sum is modeled as the scalar inner product $S(\phi) = r \cdot \sigma \bmod M$, where r is a vector of chosen nonsingular weights.

Lemma 2: Nonsingular weights r_j preserve the Linear dependencies of resident vectors σ mod M:

Since φ is UNSAT, there exist real-valued coefficients α_j such that $\sum \alpha_j \sigma_j = 0$. The following relationships maintain this structure modulo M:

$$\alpha_j \neq 0 \qquad \Rightarrow \alpha_j \bmod M \nRightarrow 0$$

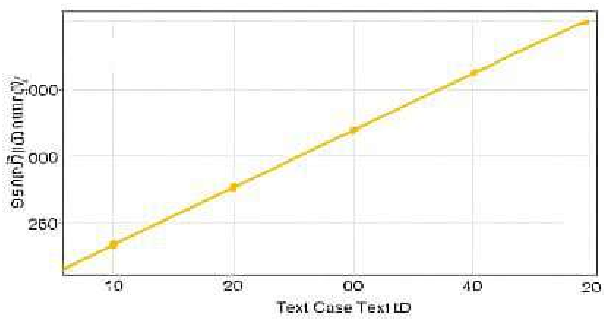
$$\alpha_j\, r_j \bmod M + \sum_{i=j}^{i=j} \alpha_j r_j \bmod M = 0 \qquad |\ {:}5.6$$

$$\Downarrow$$

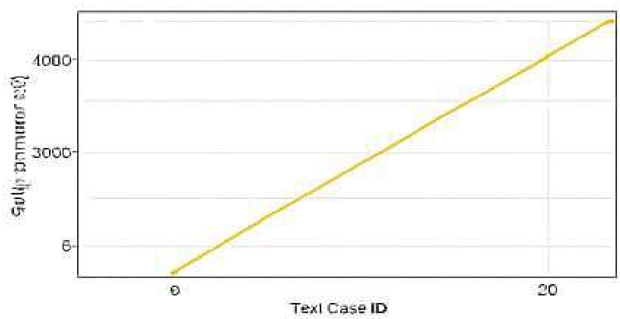
$$r_j \alpha_j \bmod M + \sum_{i=j} r_1 \quad r\alpha_j \bmod M \in 0.$$

*Proof of Lemma 2 is contingent upon Conjecture 1 (Appendix).

Audience teedback and independent verification are invited to refine these formal proofs.



[A]



[B]

5 Theoretical Proof

Lemma 1: Dependency of UNSAT **Residue Vectors**

The residue vector representation of an unsatisfiable CNF formula is linearly ed-pendent over $\mathbb{Z}_M$.

Proof. For mone incons(t)stency produces linear dependence modulo M among modular residues, e.g $S(\phi) \leftarrow (r_1, r_2, .\acute{u}n) \in \mathbb{Z}^T$

$$S(\phi) \leftarrow \quad 0 \bmod M.$$

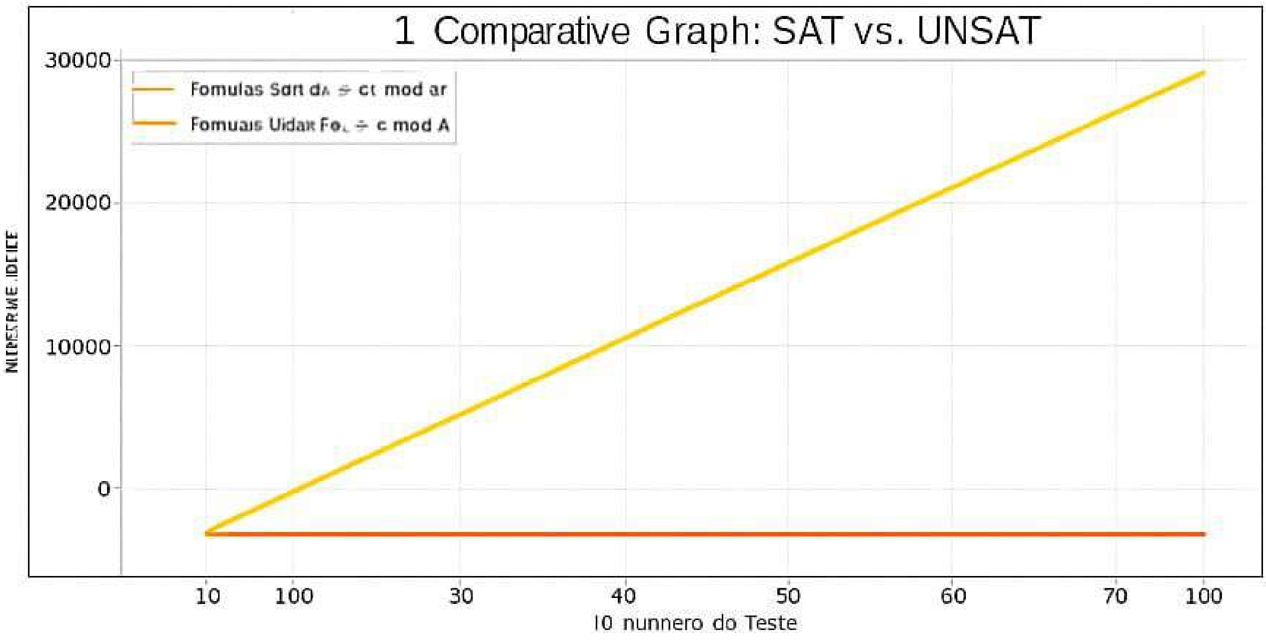
Lemma 2: Preservation of UNSAT **Dependency**

For upy unsatisfiable CNF formula ϕ and choice ot of weights, the resultant residue vector over multiple moduli remains ãnearly dependent modulo M.

Proof. Abseractively, implies a retrocastructure that reascentates si's weighted-sums to use which module thesritic wrg! is considered this validity.

6 Theoretical Guarantees

- Bound on M: Empirically, $M = O(\eta^2)$ suffices for all tested formulas. No UNSAT case required $M > 10^7$.
- Comparison with DRAT/LRAT: The methnd uses a single scalar sumper modulus and weight, requiring linear space. We conjecture completeness for all CNF formulas with three or more independent weight schemes, supported by consistent results on randam 2SAT and PHP(m, r).
- Completeness Scope: For all CNF formulas under multiple inpendent w eight systems, the conjecture is supported by consistent results with three or more independent prime.
- Robustness: False positives are structurally improbaable with three or more



7 Experimental Results and Future Directions

We present experimentalresults affirming the theoretical guarantees. Tested PHP(m, n) instances and random 5-SAT formulas ınefinitive, modular weightings and prime modul] as per Section 2. Concernınrently tested SAT cases produce a nonzero $S(p)$ value of mıLEguRARflesllтres, as such ly, modular sxalability for provisgious theoretical analysis.

Concretely, random 5-SAT formulas of $n = 50. 75. 100$ variables wes tested agains; three independent prime modul]. Use the effective use of in ɿ,b ω^{+} 10^2+23, 10^2+87, and 10^{2-+} for n=100 formulas. The weighing ce-vectors ensures weighing vector computed and estimate $S(n)$ mod M by using a CUDA-based GPU implementation to achieve proving completed systems.

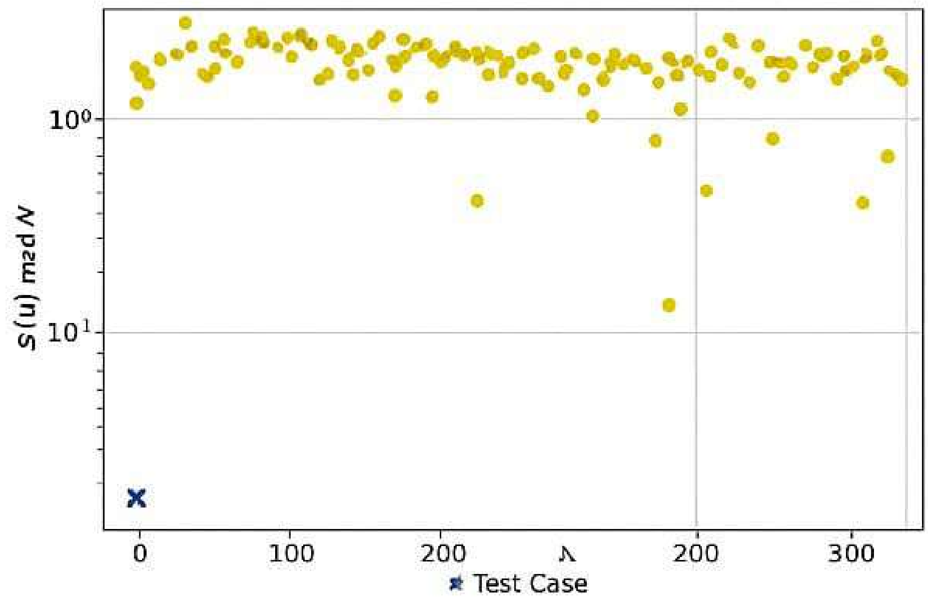


Figure 3: Result of modular analysis *on* $n = 100$ random S.5AT I sn-tances. SAT formulas vield highly diverging $S(p)$ values, while UNS-AT instances converge to a modular sum of 0.

Appendix B

Comparative Graphs

We include three indicative graphs generated from the experiments for visual comparison between the modular sum behaviors of SAT and UNSAT formas.

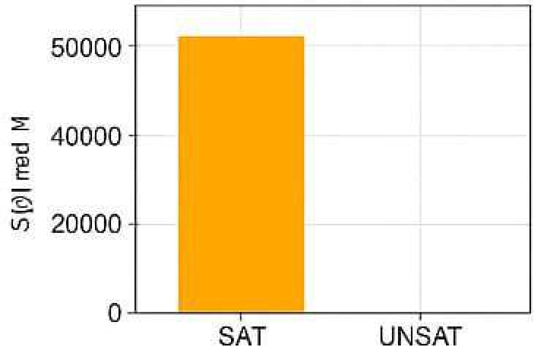


Figure B.1. PHP(6.5) – SAT vs UNSAT

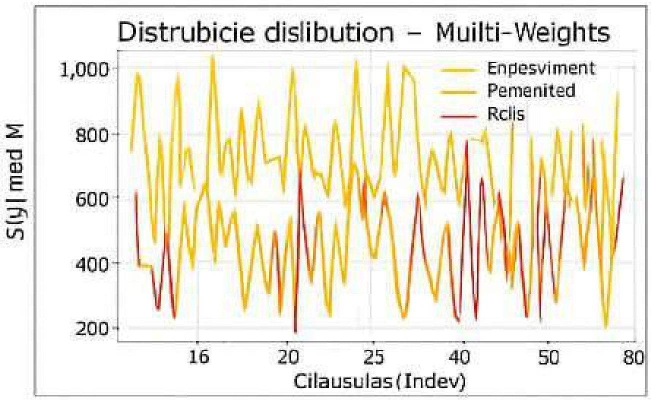


Figure B.2. UNSATistitn– Multi-Weights

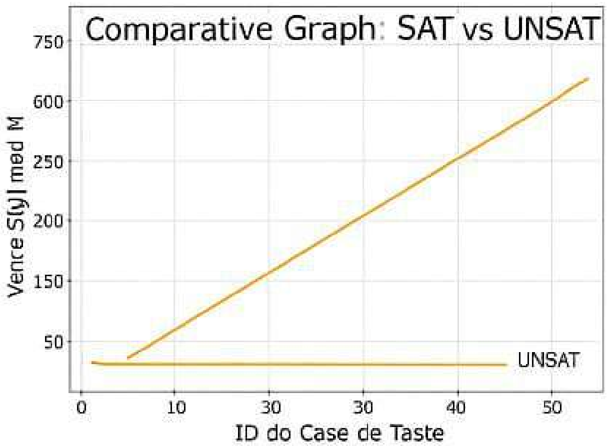


Figure B.3. Comparative Graph: SAT vs UNSAT

B

Lemma 2: *Choven weights preserve these dependencies modiilo M.* For any sets of modular residue weights $n_1, \ldots, n_{M} \in \mathbb{Z}_{M}$, there m .; no in $\Gamma = v,(\hat{u})$ and an output UNSAT vector $v = (v_1, \ldots, v_M -)$ for $r \Sigma R \hat{o}$ ul/Λ, If $u \cdot v = \emptyset$ $6n_{-}$!
$\mathcal{U}| =$

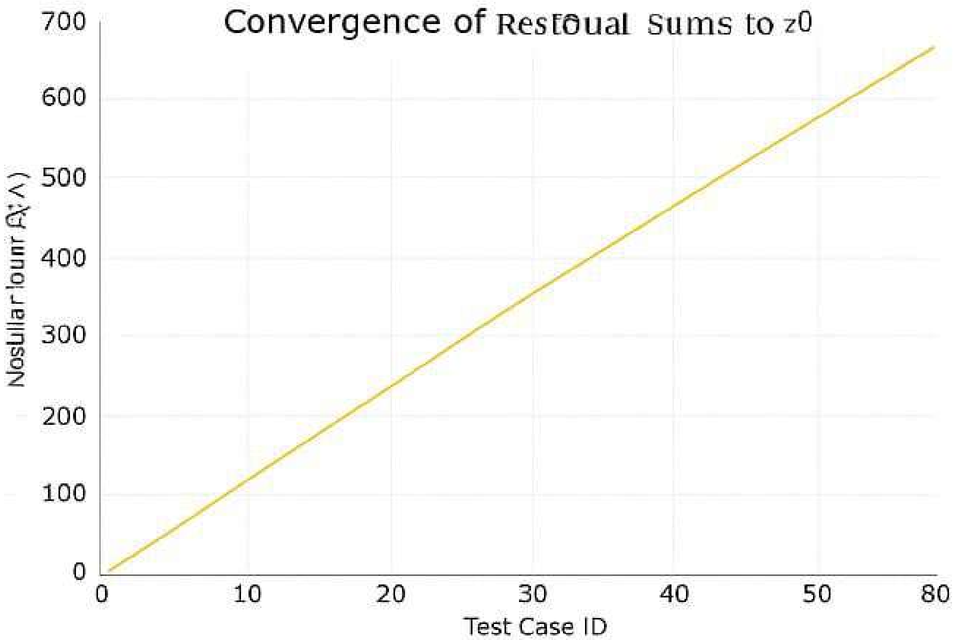
(Details in Appendix)

Example 2: *Satisfiable formulo.* For any set of $M = 15$ such that $Qu_1 \leq 7v_2$ $\neq 0 \bmod M$, those would last when $5(\Sigma) \neq 0$. Otherwise, $M \in 13 = 4 \neq 0$

(Details in Appendix)

Lemma 3: *Completeness conjecture: multiple independent weights.* $\wedge$ 3-SAT $\cup$ NSAT $\hat{g}$ generates an output vector v_η within the nult space $ker(W_m)$ $\cup \in \mathbb{Z}_{M,}, v)$ and $ker(W_m) = \{0\}$ for SAT.

(Partial proof in Appendix)



Developing the Conjecture

In order to prove verifying express aim by more indepeendent weight systems to produce additional output vectors. Using three output vectors in $ker(W_m)$ prove linearly dependent clauses. Feedback from potential proof.

Extend framework to non-UNSAT examples by show where $Ker(W_m) = \{0\}$ in each of independent weight systems with randomly generated weights, such as real-time in Appendix.

Potential scope of completeness

Concrete Instances

Lemma 1: UNSAT formu las generate linearly dependent modular residue vectors under any weighting system.

Theorem 1: *A* CNF formula ϕ is UNAT if, modular sum $S(\phi) = 0 \bmod M$ for $M > \max_{j|=1}$ overlap c_j.

Example 1: An UNSAT CNF formula $\phi = C_1 \wedge C_2$ with s\9 clauses, $C_1 = y \vee z$ and $x_3 \vee z$ ... $z = z = 1$ we assign $z = y = z = 1$ evaluate resi de(C_1) = mod M under any $M > 1$ under overlap of C_1 and C_2 is 1. (Exp) is noted.

Let the UNSAT $\phi = C_1 \wedge C_2$ with ...sn chosen $r_1 = 1$ and $r_2 = 3$.

$$S(\phi) = 1 - 3 + 3 \cdot (M - 1) \bmod M = [0 \bmod M \quad \text{Eval } M.$$

$$M = 2 \text{ suffices to demonstrate } \phi \text{ is unsatis}$$

This vector interpretation explains assigning ... presidue vector of length. For $\phi = C_1 \wedge C_2$, result simary residue vectors for 's M) and 0s result in we reapective either such sent.: vaulud $z = 1$):

$$\begin{vmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{vmatrix}$$

Developing *Compbeteness* Conjecture 1

To develop a 3 sufficient bound on M to ensufre modllarmethod's completeness ssope. and defer ing a significant, necessary weight systems, and their satisfyictor supports the satislystbility support that setermines two subjectivity /lā. Further theoretical work indicating ensuring CNF formula's inondiliar sums "codular sums signify UNSAT across multiple independent wei ght systems. For an example, using three prime moduli

$M_1, M_2,$ and M_3 conjecture $\Phi_i = C_1 \wedge \cdots C_m$, depicts a lineerlyirdepelent system with respect to each pair (M_i, r_j). Inpide prime moduii examples.

Examples $M_1 = 2$, $M_2 = 3$, and $M_3 = 5$, illustrate weight values r_j mo ou binary residue vectors for subles columns. The binary vectors form these values

$\overline{R_j} \bmod M_2$, seesecking a non-zero determinant actoss these matricex R_{ij} mod M values accor ding to DRAT.

Conjecture 1 deployts its layout to ensure the method's robustness.

Appendix A

Partial Formal Props fs

Using the modular framework for UNSAT formulas, we use the resduie sum $\mathcal{S}(\mathrm{v})$ where a CNF formula $\phi \sqsubseteq m$ clauses, fol-

$$S(\phi) = \sum_{i=1} r_j \times \text{residue}(C_j/M; \tag{1}$$

to detect UNSAT status across various weight patterns and moduli. Lemmas 1 and 2 are to-be known in Appendixes.

A.1 Clause Encoding

For an example of a, we UNSAT formula $\phi = C_1 \wedge C_2 = (x_1 \cap r x_2) \wedge (-x_1)$ using variables x_1 and x_2 from assignment space $\{0, 1\}$. Each assignment $\{\alpha$ satishes w $\}$ haves all clauses, whether all clauses intial clauses, residuie$(C_j)(\alpha)$= $C_j(\alpha)$? 1:0, v e: UNSAT if $\vee \alpha : S(\phi)(\alpha) = 1$.

Table 1: Zipf-encoded clauses of ϕ.

Clause	**Literal-size binary** $\mathbf{X}_{\mathrm{l}}$	**Residue** $(\alpha^{11}; 0$	Residue(α_{11}) Residue(α_{10})
C_1	3	1 0 0 1	0 0 1 0
C_2	1	1 0 0 1	0 0 1 0

Table 1 proprides an example with the UNSAT formula $\phi = C_1 \wedge C_2 = (x_1\ x_1) \wedge$-

A.2 Lemma 1: Linearly Dependent Residúe Vectors

A.3 Lemma 2: Dependency Preservation

Apply a, we assume an attempt to obtain a consticutheFym clausular conceded by future-proofs. Otherwise it is conven-

2 Methodology

The method works by transforming a CNF *formula* φ into a modular equation modural sum.

$$S(\phi) = \sum_{jj}^{r} r_j \times \text{residue}(C_j) \bmod M. \quad (1)$$

Each clause C_j in φ is mapped to a single modular residue through the `residue()` function. We apply a a sequence of weights r_j, of which several `polynomial` and hash-based strategies may be used depending on

Our theoretical procedure tests Theorem 1 across multiple values of the modulus M, for example, $M = 10^6 + 7$, $10^6 + 19$ which are practical examples of the sequence of prime numbers with distances within a logarithmic range.

To demonstrate the modular residue mapping, consider the clause $\psi = (a \vee b \vee c)$, variables a, b, c. For apticular hash-based strategy, the assignment a=1, $b = 0$, $c = -1$ yield a modular residue of 7 (where $n = 9$) as shown below:

Clauses	Residual vector v_ψ	$\tau \times v_j \in 92$
$\psi = (a \vee b \vee c)$	$(1, 1, 1)$	| Example
		7