

دانشگاه صنعتي امیرکبیر  
(پلی تکنیک تهران)

دانشكده مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه کارشناسی‌ارشد

گرایش امنیت اطلاعات

اجرايConcolic براي تشخيص آسيب‌پذيري تزريق به برنامه‌هاي کاربرديِ گوشي‌هاي هوشمند

نگارش

احسان عدالت

استاد راهنما

جناب آقای دکتر بابک صادقیان

آذر 96

صفحه فرم ارزیابی و تصویب پایان نامه- فرم تأیید اعضاء كميته دفاع

در این صفحه فرم دفاع یا تایید و تصویب پایان نامه موسوم به فرم کمیته دفاع- موجود در پرونده آموزشی- را قرار دهید.

نکات مهم:

* نگارش پایان نامه/رساله باید به زبان فارسی و بر اساس آخرین نسخه دستورالعمل و راهنمای تدوین پایان نامه های دانشگاه صنعتی امیرکبیر باشد.(دستورالعمل و راهنمای حاضر)
* رنگ جلد پایان نامه چاپي كارشناسي، كارشناسي ارشد و رساله دكترا بايد به ترتيب مشكي، طوسي و سفيد رنگ باشد.
* چاپ و صحافی پایان نامه/رساله بصورت پشت و رو(دورو) بلامانع است و انجام آن توصيه مي شود.

اينجانب احسان عدالت متعهد مي‌شوم كه مطالب مندرج در اين پايان نامه حاصل كار پژوهشي اينجانب تحت نظارت و راهنمايي اساتيد دانشگاه صنعتي اميركبير بوده و به دستاوردهاي ديگران كه در اين پژوهش از آنها استفاده شده است مطابق مقررات و روال متعارف ارجاع و در فهرست منابع و مآخذ ذكر گرديده است. اين پایان نامه قبلاً براي احراز هيچ مدرك هم‌سطح يا بالاتر ارائه نگرديده است.

در صورت اثبات تخلف در هر زمان، مدرك تحصيلي صادر شده توسط دانشگاه از درجه اعتبار ساقط بوده و دانشگاه حق پيگيري قانوني خواهد داشت.

كليه نتايج و حقوق حاصل از اين پایان نامه متعلق به دانشگاه صنعتي اميركبير مي‌باشد. هرگونه استفاده از نتايج علمي و عملي، واگذاري اطلاعات به ديگران يا چاپ و تكثير، نسخه‌برداري، ترجمه و اقتباس از اين پایان نامه بدون موافقت كتبي دانشگاه صنعتي اميركبير ممنوع است.   
نقل مطالب با ذكر مآخذ بلامانع است.

احسان عدالت

امضا

**در صورت تمایل این صفحات نیز اضافه شود: (اختیاری)**

* **صفحه تقديم**

نويسنده پايان‏نامه، درصورت تمايل مي‏تواند برای سپاسگزاری پايان‏نامه خود را به شخص يا اشخاص و يا ارگان خاصی تقدیم نماید.

* **صفحه تقدير و تشكر**

نويسنده پايان‏نامه مي‏تواند مراتب امتنان خود را نسبت به استادراهنما و استادمشاور و یا ديگر افرادي كه طي انجام پايان‏نامه به نحوي او را یاری و یا با او همكاري نموده‏اند ابراز دارد.

چكيده

در اين قسمت چكيده پایان نامه نوشته مي‌شو‌د‌.‌ چكيده بايد جامع و بيان‌كننده‌ خلاصه‌اي از اقدامات انجام‌شده باشد. در چكيده باید از ارجاع به مرجع و ذكر روابط رياضي، بيان تاريخچه و تعريف مسئله خودداري ‌شود.

واژه‌های کلیدی:

کلیدواژه اول، ...، کلیدواژه پنجم (نوشتن سه تا پنج واژه کلیدی ضروری است)

|  |  |
| --- | --- |
| فهرست مطالب | صفحه |

[فصل اول مقدمه 1](#_Toc465667638)

[فصل دوم مشخصات یک پایان نامه و گزارش علمی 3](#_Toc465667639)

[2-1- برخورداری از غنای علمی 4](#_Toc465667640)

[2-2- ارجاع به‌موقع و صحیح به منابع دیگر 4](#_Toc465667641)

[2-3- ساده‌نویسی 4](#_Toc465667642)

[2-3-1- وحدت موضوع 5](#_Toc465667643)

[2-3-2- اختصار 5](#_Toc465667644)

[2-3-3- رعایت نكات دستوري و نشانه‌گذاري 5](#_Toc465667645)

[2-3-4- توجه به معلومات ذهنی مخاطب 5](#_Toc465667646)

[2-3-5- رعایت مراحل اصولی نگارش 6](#_Toc465667647)

[فصل سوم نگارش صحيح 7](#_Toc465667648)

[3-1- فارسي‌نويسي 8](#_Toc465667649)

[3-2- رعایت املاي صحيح فارسي 9](#_Toc465667650)

[3-3- رعایت قواعد نشانه‌گذاري 9](#_Toc465667651)

[3-3-1- ويرگول 9](#_Toc465667652)

[3-3-2- نقطه 9](#_Toc465667653)

[3-3-3- دو نقطه 10](#_Toc465667654)

[3-3-4- گيومه 10](#_Toc465667655)

[3-3-5- نشانه پرسشی 10](#_Toc465667656)

[3-3-6- خط تیره 10](#_Toc465667657)

[3-3-7- پرانتز 11](#_Toc465667658)

[فصل چهارم سبك ها و قلم ها 12](#_Toc465667659)

[4-1- قلم‌هاي فارسي 13](#_Toc465667660)

[4-2- قلم‌هاي انگلیسی 14](#_Toc465667661)

[4-3- فرمول‌ها(روابط رياضي) 15](#_Toc465667662)

[4-4- فاصله‌هاي افقي و عمودي 16](#_Toc465667664)

[4-4-1- فاصله كلي از چهار طرف كاغذ 16](#_Toc465667665)

[4-4-2- فاصله خط‌ها 16](#_Toc465667666)

[4-4-3- فاصله‌هاي تفكيك‌كننده 16](#_Toc465667667)

[4-5- فواصل بين كلمات 17](#_Toc465667668)

[4-6- جدانوشتن كلمات بدون گذاشتن فاصله بين آنها 17](#_Toc465667669)

[4-7- فهرست گزارش، فهرست شكل‌ها و فهرست جداول 17](#_Toc465667670)

[4-8- سربرگ و ته‌برگ (Header and Footer) 18](#_Toc465667671)

[4-9- جداول، منحني‌ها، شكل‌ها و مراجع 18](#_Toc465667672)

[4-10- ارجاع به جداول، شكل‌ها، روابط، مراجع و بخش‌ها 19](#_Toc465667673)

[فصل پنجم بررسي ساختار پایان نامه 20](#_Toc465667674)

[5-1- بررسي سرفصل‌ها 21](#_Toc465667675)

[5-2- بررسي ساختار كلي 21](#_Toc465667676)

[5-3- بررسي مفهومي 21](#_Toc465667677)

[5-4- مطالعه مفهومي و جمله‌بندي 22](#_Toc465667678)

[5-5- تنظیم بندها 22](#_Toc465667679)

[5-6- بررسي قواعد نگارشي 23](#_Toc465667680)

[5-7- بررسي روابط 23](#_Toc465667681)

[5-8- بررسي شكل‌ها 24](#_Toc465667682)

[5-8-1- بررسي كيفيت شكل و تطابق عنوان آن 24](#_Toc465667683)

[5-8-2- بررسي تطابق روابط، برنامه و شكل 24](#_Toc465667684)

[5-9- بررسي جداول 24](#_Toc465667685)

[5-9-1- بررسي كيفيت جدول و تطابق عنوان آن 24](#_Toc465667686)

[5-9-2- بررسي تطابق روابط، برنامه و جدول 25](#_Toc465667687)

[5-10- به‌روز‌رساني مراجع 25](#_Toc465667688)

[5-11- صفحه‌بندي 25](#_Toc465667689)

[5-12- سربرگ و ته‌برگ‌ها 25](#_Toc465667690)

[فصل ششم جمع‌بندي و نتيجه‌گيري و پیشنهادات 27](#_Toc465667691)

[منابع و مراجع 29](#_Toc465667692)

[پيوست‌ها 31](#_Toc465667693)

|  |  |
| --- | --- |
| فهرست اشكال | صفحه |

[شكل ‏4‌-‌‌1- فرايند كواكستروژن . 18](#_Toc276969410)

|  |  |
| --- | --- |
| فهرست جداول | صفحه |

[جدول ‏4‌-‌1- قلم‌هاي فارسي 13](#_Toc276969411)

[جدول ‏4‌-‌2- قلم‌هاي انگلیسی. 14](#_Toc276969412)

[جدول ‏4‌-‌3- قلم و سبك فرمول‌ها. 15](#_Toc276969413)

[جدول ‏4‌-‌4- اندازه فرمول‌ها. 15](#_Toc276969414)

[جدول ‏4‌-‌5- عنوان جدول. 18](#_Toc276969415)

|  |
| --- |
| فهرست علائم |

علائم لاتين

|  |  |  |
| --- | --- | --- |
|  |  | ارتفاع |
|  |  | طول موج توربولانس |
|  |  | پريود توربولانس |
|  |  | سرعت تعادل وسيله پرنده |
|  |  | مولفه سرعت تندباد در راستاي محور طولي دستگاه مختصات بدني نسبت به اينرسي |

علائم يوناني

|  |  |  |
| --- | --- | --- |
|  |  | چگالي طيفي قدرت توربولانس |
|  |  | شدت توربولانس |
|  |  | بسامد توربولانس |
|  |  | بسامد فاصله‌اي |
|  |  |  |

بالا‌نويس‌ها

|  |  |  |
| --- | --- | --- |
|  |  | دستگاه مختصات بدني |

زيرنويس‌ها

|  |  |  |
| --- | --- | --- |
|  |  | تندباد (گاست) |

# فصل اول مقدمهمقدمه

فصل مقدمه یک پایان نامه، با بیان نیاز موضوع، تعريف مسئله و اهمیت آن در یک یا چند بند (پاراگراف) آغاز مي‌شود[[1]](#footnote-1) و با مرور پيشينه موضوع (سابقه کارهای انجام‌شده پیشین که ارتباط مستقیمی با مسئله مورد بررسی دارند) ادامه مي‌يابد. سپس در یک یا دو بند توضیح داده مي‌شود كه در این پایان نامه، چه ديدگاه يا راهكار جدیدي نسبت به مسئله (موضوع) مورد بررسي وجود دارد. به‌عبارت دیگر نوآوری‌ها به‌صورت کاملاً شفاف و صریح بیان می‌شود. در ادامه ممکن است به نتايج بدست‌آمده نیز به‌طور مختصر و کلی اشاره ‌شود. در آخرین بند از مقدمه به محتواي فصل‌هاي بعدي پایان نامه به‌اختصار اشاره مي‌شود.

# فصل دوم اجرای Concolicاجرای Concolic

یکی از روش‌های آزمون نرم‌افزار اجرای Concolic است. در این روش به صورت هم‌زمان کد برنامه را هم به صورت عینی و هم به صورت نمادین اجرا می‌کنند. اجرای نمادین باعث می‌شود پوشش مناسبی از کد بدست بیاید ولی در عین حال ممکن است مسیری از برنامه با اجرای نمادین صرف، قابل دسترس نباشد که وجود اجرای عینی این مسئله را حل می‌کند. در این فصل قصد داریم اجرای Concolic و کارهای صورت گرفته در این حوزه را مورد بررسی قرار دهیم. در انتهای فصل کاربرد این روش در برنامک‌های اندرویدی نیز مورد بررسی قرار خواهد گرفت.

## بیان اجرای نمادین و Concolic با مثال

برای توضیح روش اجرای نمادین و Concolic از شکل ‏2‑2 که شامل یک برنامه ساده است استفاده خواهیم کرد. تفاوت دو اجرای نمادین و Concolic در این است که در اجرای Concolic علاوه بر اجرای نمادین به صورت هم‌زمان برنامه به شکل عینی نیز اجرا خواهد شد.

ابتدا اجرای نمادین برنامه شکل ‏2‑2 را بررسی می‌کنیم. وقتی در اجرای نمادین متغیری نمادین در نظر گرفته می‌شود (خط ۱۱ و ۱۲) به این معنی است که آن متغیر نماینده تمام مقادیر ممکن برای آن نوع است. مثلا متغیر x نماینده تمام مقادیر ممکن برای نوع int است. این مقدار را با حرف بزرگ نشان خواهیم داد. مثلا مقدار نمادین متغیر x را با X نشان می‌دهیم. برنامه با مشخص شدن این مقادیر اجرا می‌شود. در خط ۱۳ برنامه متغیر y با عمل انتساب مقدار Z+6 را خواهد پذیرفت که همان طور که مشخص است مقداری نمادین است. سپس در خط ۱۴ تابع testMe با مقادیر نمادین X و Z+6 فراخوانی می‌شود.

1: testMe(int x, int y){

2: if(y>5){

3: assert(false);

4: }else{

5: if(x\*x\*x > 10){

6: assert(false);

7: }

8: }

9: }

10: void main ( ){

11: int x = symbolic\_input();

12: int z = symbolic\_input();

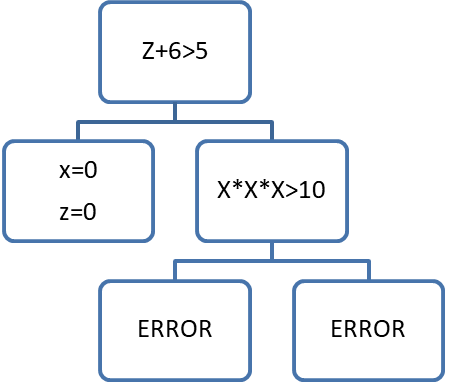
13: int y = z+6;

14: testMe(x,y);

15: }

شکل ‏2‑2 نمونه برنامه ساده

اجرای نمادین در مواجه با دستورات شرطی از قبیل if، شرط مربوط به آن را به صورت یک عبارت منطقی به عنوان شرط مسیر[[2]](#footnote-2) نگهداری می‌کند. همان طور که مشخص است دستورات شرطی موجود در برنامه موجب می‌شوند تا مجموعه دستورهایی که قرار است بعد از آن اجرا شوند، تصمیم‌گیری شوند. شرط مسیر عبارتی است که از عطف[[3]](#footnote-3) شرط‌های دستورهای شرطی موجود در آن مسیر بدست می‌آید. شرط مسیر در ابتدا مقدار درست[[4]](#footnote-4) دارد. برای مثال در خط ۲ برنامه، شرط y > 5 که معادل Z+6 > 5 است به شرط مسیر اضافه می‌شود و داریم: PC=(Z+6>5). اگر این شرط برقرار باشد، خط ۳ اجرا می‌شود. برای اینکه پوشش کامل مسیرهای برنامه بدست آید، یعنی خط‌های ۵ و ۶ هم اجرا شود، شرط مسیر باید PC=(Z+6<=5) باشد. در اجرای نمادین تمام حالت‌های ممکن برای شرط مسیر در نظر گرفته می‌شود. مجموعه شرط‌های مسیر ممکن در کنار هم درخت اجرا[[5]](#footnote-5)ی برنامه را می‌سازند. در شکل ‏2‑1 درخت اجرای برنامه نمونه را می‌بینید.



شکل ‏2‑1 درخت اجرای اجرای نمادین برنامه نمونه

برای تولید موردآزمون برای هر مسیر، شرط مسیر مربوط به آن، به ابزار «حل کننده قید[[6]](#footnote-6)» داده می‌شود. این ابزارها با دریافت یک عبارت منطقی، مقادیر متناظر با هر متغیر در آن عبارت را پیدا می‌کنند که به ازای آنها کل عبارت درست خواهد بود. مثلا به ازای x=0 و y=0 عبارت PC=Z+6>5 درست است و خط ۳ برنامه اجرا می‌شود. حل‌کننده‌های قید دارای توان محدودی هستند برای مثال توانایی حل عبارت‌های غیرخطی مثل X\*X\*X>10 را ندارند. در نتیجه با اجرای نمادین نمی‌توان موردآزمونی تولید کرد که به ازای آن خط ۶ برنامه اجرا شود.

در روش Concolic متغیرها علاوه بر شکل نمادین به صورت مقدار عینی[[7]](#footnote-7) نیز در نظر گرفته می‌شوند. مقدار عینی در ابتدا به صورت دلخواه انتخاب می‌شود. برای مثال در این برنامه مقدار اولیه عینی x=1 و z=1 به صورت دلخواه انتخاب می‌شود. شرط مسیر استخراج شده با این ورودی‌ها PC=(Z+6>5) خواهد بود. برای تولید ورودی عینی جدید مکمل شرط مسیر یعنی PC=(Z+6<=5) به حل‌کننده قید داده می‌شود. مقدار جدید z=-2 و x=1 خواهد بود که با آن شرط مسیر PC=(Z+6<=5) and (x\*x\*x<10) تولید می‌شود. همان طور که گفته شد، حل‌کننده قید توانایی حل عبارت‌های غیر خطی مثل (x\*x\*x<10) را ندارد. در این جا اجرای Concolic با قرار دادن یک مقدار دلخواه به جای x به اجرا ادامه می‌دهد. اگر مقدار دلخواه موجب درست شدن شرط مسیر شود، خطا در برنامه کشف خواهد شد. مثلا x=3 و z=-2 باعث می‌شود برنامه به خط ۶ برسد.

## چالش‌های اجرای Concolic

اجرای Concolic با چالش‌های مختلفی روبه‌رو است که در ادامه گفته خواهند شد. هر یک از این چالش‌ها به نحوی سعی شده است که در کارهای گذشته حل شوند که در ادامه فصل بیان خواهند شد.

چالش‌های اجرای Concolic عبارتند از:

* **حافظه**: موتور اجرای نمادین چگونه اشاره‌گرها، آرایه‌ها و ساختمان داده‌ها را پردازش می‌کند؟ آیا می‌تواند ساختمان‌داده‌های پیاده‌سازی شده برنامه نویس را هم پردازش کند؟
* **محیط**: برنامه مورد آزمون ممکن است که با محیط خود و متغیرهای موجود در آن تعامل داشته باشد. مثلا برنامک‌های اندرویدی که پیوسته با سیستم عامل در ارتباطند و قطعه کدهای مختلف موجود در آن را اجرا می‌کند. همچنین سیستم فایل، شبکه، تعاملات کاربر با برنامه و غیره هم از این دست هستند. موتور اجرای نمادین باید برای این موارد راه حل داشته باشد. پس اجرای نمادین در پلتفرم‌های مختلف متفاوت خواهد بود.
* **حلقه‌ها**: موتور اجرای نمادین باید در مورد تعداد دفعات اجرای بدنه یک حلقه تصمیم‌گیری کند. ممکن است یک حلقه شرط خاتمه نداشته باشد در نتیجه آزمون برنامه دچار انفجار مسیر خواهد شد.
* **انتخاب مسیر و مسئله انفجار مسیر**: انتخاب اینکه کدام یک از مسیر‌های برنامه اجرا شود و هیوریستیک انتخاب کننده آن بسیار مهم است. برنامه‌های واقعی مسیرهای زیادی دارند که اجرای همه آنها موجب انفجار مسیر شده و هیچگاه فرایند آزمون تمام نمی‌شود.
* حل‌کننده‌های قید: حل‌کننده‌های قید محدودیت‌های زیادی دارند و نمی‌توانند همه قیدها را حل کنند. نیاز است تا با روش‌هایی این قیدها و تعداد آنها کاهش یابد و ساده شوند.
* **کدهای باینری**: در دنیای واقعی برنامه‌هایی وجود دارند که کد آنها در دسترس نیست و نیاز است تا این برنامه‌ها را با وجود کد باینری آزمود هر چند که وجود کد منبع و سطح بالای آنها تحلیل را آسان‌تر می‌کند.

## انواع اجرای Concolic

در این حوزه اجرای Concolic به دو صورت آفلاین و آنلاین و یا ترکیب این دو صورت می‌گیرد. منظور از اجرای Concolic آفلاین است که در هر بار اجرا، یک مسیر انتخاب می‌شود این موضوع باعث می‌شود استفاده از حافظه کم باشد ولی تعداد زیادی از دستورات و کدها بارها به صورت تکراری اجرا می‌شوند. در اجرای آنلاین برخلاف آفلاین با یک بار اجرا تمام مسیرهای موجود اجرا می‌شوند. در این حالت با استفاده از دستور fork بر سر هر دستور شرطی، هر دو شاخه موجود همزمان اجرا می‌شوند. مزیت این روش در این است که هر دستور فقط یکبار اجرا می‌شود ولی استفاده از حافظه در آن به شدت زیاد است.

در برخی از کارها سعی شده است است که از ترکیب این دو روش استفاده شود تا مزیت هرکدام را در خود داشته باشد. در این حالت «ترکیبی» تا زمانی که استفاده از حافظه به حد معین شده خود نرسیده است، برنامه به صورت آنلاین اجرا می‌شود. بعد از آن اجرا آفلاین می‌شود تا زمانی که به اندازه کافی حافظه آزاد شود تا دوباره اجرا به شکل آنلاین ادامه پیدا کند.

## کارهای گذشته

در ادامه کارهایی را بیان خواهیم کرد که در مورد اجرای Concolic از سال ۲۰۰۵ تا کنون انجام شده است. در مورد هر کار ویژگی‌های خاص آن و بهبودی که در مورد هر چالش داشته است را توضیح خواهیم داد. در جدول ‏2-1 کارهای گذشته شاخص آمده‌اند.

جدول ‏2-1 کارهای گذشته

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ویژگی** | **نوع** | **پلتفرم** | **زبان برنامه مورد آزمون** | **ابزار** | **سال** |  |
| عمق‌اول | آفلاین | کامپیوتر شخصی | C | DART | ۲۰۰۵ | ۱ |
| مدل‎سازی حافظه، عمق‌اول کراندار، بهینه‌سازی | آفلاین | کامپیوتر شخصی | C | CUTE | ۲۰۰۵ | ۲ |
| CUTE، همروندی | آفلاین | کامپیوتر شخصی | جاوا | jCUTE | ۲۰۰۶ | ۳ |
| مدل‎سازی حافظه، عمق‌اول و سطح‌اول ترکیبی، بهینه‌سازی، STP | آنلاین | کامپیوتر شخصی | C | EXE | ۲۰۰۶ | ۴ |
| CUTE، ترکیب اجرای دلخواه و Concolic | آفلاین | کامپیوتر شخصی | C | Hybrid | ۲۰۰۷ | ۵ |
| DART، ترکیب Compositional و Concolic | آفلاین | کامپیوتر شخصی | C | Compositional | ۲۰۰۷ | ۶ |
| EXE، بهینه‌سازی انتخاب مسیر و حل‌کننده قید، متن‌باز | آنلاین | کامپیوتر شخصی | C | KLEE | ۲۰۰۸ | ۷ |
| متن‌باز، بهینه‌سازی کارهای گذشته | آفلاین | کامپیوتر شخصی | جاوا | jFUZZ | ۲۰۰۹ | ۸ |
| ترکیب وارسی مدل و اجرای نمادین | آفلاین | کامپیوتر شخصی | جاوا | SPF | ۲۰۱۰ | ۹ |
| متن‌باز، SMT، معماری برنامه نویسی سوکت | آفلاین | کامپیوتر شخصی | جاوا | LCT | ۲۰۱۱ | ۱۰ |
| آسیب‌‌پذیری سرریز بافر، خاصیت ایمنی | آفلاین | کامپیوتر شخصی | باینری و C | AEG | ۲۰۱۱ | ۱۱ |
| متن‌باز، رخدادمحور | آفلاین | Phone | اندروید | ACTEVE | ۲۰۱۲ | ۱۲ |
| آسیب‌‌پذیری سرریز بافر، قالب رشته، مدل‌سازی‌حافظه | ترکیبی | کامپیوتر شخصی | باینری | MAYHEM | ۲۰۱۲ | ۱۳ |
| ثبت-بازاجرای انتخابی، مقادیر سایه | آفلاین | وب | جاوا اسکریبت | Jalangi | ۲۰۱۳ | ۱۴ |
| کشف نشت حریم خصوصی | آفلاین | Phone | اندروید | AppIntent | ۲۰۱۳ | ۱۵ |
| استفاده از کلاس‌های Mock،  گراف فراخوانی توابع | آفلاین | Phone | اندروید | SIG-Droid | ۲۰۱۵ | ۱۶ |
| Concolic + Call Flow Graph | آفلاین | Phone | اندروید | Condroid | ۲۰۱۵ | ۱۷ |
| ترکیب instrumented-Genetic-Fuzzer با Concolic | ترکیبی | کامپیوتر شخصی | باینری | Driller | ۲۰۱۶ | ۱۸ |
| تشخیص آسیب‌پذیری سرریز پشته | آفلاین | کامپیوتر شخصی | باینری | Smart Fuzzer\_1 | ۲۰۱۶ | ۱۹ |
| تشخیص آسیب‌پذیری سرریز هیپ | آفلاین | کامپیوتر شخصی | باینری | Smart Fuzzer\_2 | ۲۰۱۶ | ۲۰ |

در ادامه به توضیحی مختصر در رابطه با هر مقاله می‌پردازیم:

1. در سال 2005 اولین ابزار با روش Concolic آفلاین به نام Dart [1] ارائه شد. این ابزار از lp\_solve به عنوان حل‌کننده قید استفاده می‌کند. همچنین محدود به زبان C است و مدل‌سازی حافظه ندارد. علاوه بر آن از برنامه‌های هم‌روندی پشتیبانی نمی‌کند. از جست‌وجوی DFS برای انتخاب مسیرها در درخت اجرا استفاده می‌کند و بهینه‌سازی برای ارسال قیدها به حل کننده قید ندارد همچنین این ابزار در حل قیدهای مربوط به اشاره‌گرها مشکل دارد.
2. در سال 2005، ابزار CUTE [2] با روش Concolic آفلاین ارائه شد که از lp\_solve استفاده ‌می‌کند. این ابزار هم محدود به زبان C است و از هم‌روندی پشتیبانی نمی‌کند. ولی مدل‌سازی حافظه دارد و از نگاشت منطقی ورودی‌ها استفاده می‌کند و مشکل قیدهای اشاره‌گر را حل کرده است. همچنین از جست‌وجوی DFS کراندار برای انتخاب مسیرها استفاده می‌کند و بهینه‌سازی برای ارسال قیدها به حل کننده قید دارد. روش‌های بهینه سازی آن عبارتند از: بررسی سریع ارضاناپذیری، حذف قیدهای معمول و حل افزایشی.
3. در سال 2006، ابزار JCUTE [3] با روش Concolic آفلاین، ارائه شد که از lp\_solve استفاده می‌کند. این ابزار محدود به زبان جاوا است ولی مدل‌سازی حافظه دارد و مانند CUTE از نگاشت منطقی ورودی‌ها استفاده می‌کند. همچنین از هم‌روندی پشتیبانی می‌کند یعنی علاوه بر ورودی‌های برنامه، زمانبند نخ‌ها هم باید به صورت خودکار برنامه‌ریزی شود. این ابزار از جست‌وجوی DFS برای انتخاب مسیرها استفاده می‌کند و مانند CUTE بهینه‌سازی برای ارسال قیدها به حل کننده قید دارد.
4. در سال 2006، ابزار EXE [4] با روش Concolic آنلاین، اراپه شد که از STP استفاده می‌کند. این ابزار محدود به زبان C است و از هم‌روندی پشتیبانی نمی‌کند. ولی مدل‌سازی حافظه دارد. حافظه را مجموعه‌ای از بایت‌های بدون نوع در نظر می‌گیرد. همچنین از جست‌وجوی DFS و BFS به صورت ترکیبی برای انتخاب مسیرها استفاده می‌کند. علاوه برآن بهینه‌سازی برای ارسال قیدها به حل کننده قید دارد. ایده‌های این ابزار در این مورد استفاده از روش کش و شناسایی زیرقیدهای مستقل و حذف زیرقیدهای بی ارتباط است.
5. اجرای هیبرید [5] به صورت ترکیبی اجرای دلخواه[[8]](#footnote-8) و Concolic را انجام می‌دهد تا بتواند از مزیت‌های هر یک استفاده کند. کار ارائه شده بروی ابزار CUTE است. ابتدا کد به صورت عینی اجرا می‌شود. هر گاه اجرا اشباع شد اجرا به Concolic تغییر میابد تا بتواند به صورت عمق‌محدود به پوشش بیشتری از کد برسد. دوباره بعد از یافتن مسیر جدید اجرا به عینی تغییر میابد. اجرای هیبرید برای برنامه‌های تعاملی مثل برنامه‌های رخدادمحور یا دارای GUI مناسب است. این اجرا همان محدودیت‌های اجرای Concolic را دارد. ممکن است به پوشش 100 درصد از کد نرسد ولی از نظر نویسندگان پوشش کامل نشانه ای برای قابل اعتماد بودن[[9]](#footnote-9) کد نیست.
6. کار مورد شش در جدول [6]، از DART به عنوان موتور Concolic استفاده می کند. هدف این کار توسعه DART برای برنامه های واقعی با تعداد خط کد بالاست به همین دلیل از تحلیل ایستای Compositional استفاده می کند که برای توابع function summery استخراج می کند و به جای اجرای هر باره یک تابع از summery آن استفاده می کند و آن را به شرط مسیر اضافه می‌کند.
7. ابزار KLEE [7] در سال 2008، با روش Concolic آنلاین ارائه شد که از STP استفاده می‌کند. این ابزار برای آزمون برنامه‌های واقعی محدود به زبان C است. مدل‌سازی محیط اجرای برنامه(سیستم فایل) و مدل‌سازی حافظه دارد. حافظه را مجموعه‌ای از بایت‌های بدون نوع در نظر می‌گیرد. ولی از هم‌روندی پشتیبانی نمی‌کند. این ابزار روش‌های انتخاب دلخواه و انتخاب برای پوشش بیشترین مسیرها را به صورت ترکیبی استفاده می‌کند. بر اساس یک سری هیوریستیک به حالت‌ها وزن اختصاص داده می‌شود و سپس به صورت دلخواه یکی از این حالت‌ها انتخاب می‌شوند. در حالت دوم، هیوریستیک‌ها بر اساس کمترین فاصله تا دستور پوشش داده نشده، بیشینه فراخوانی حالت و یا اینکه یک حالت اخیرا دستور جدیدی را پوشش داده است یا نه، محاسبه می‌شود. ترکیب این دو استراتژی باعث می‌شود هم پوشش تمامی دستورات فراهم شود و هم از گیر کردن در حلقه جلوگیری به عمل آید. برای بهینه‌سازی قید‌ها به حل کننده قید از روش‌هایی مثل روش کش استفاده می‌کند. این ابزار گسترش یافته ابزار EXE است.
8. jFuzz [] ابزار متن باز برای جاواست. نوآوری خاصی ندارد و ترکیب بهینه سازی های کارهای قبلی مثل KLEE، CUTE و غیره را در خود دارد. این ابزار بروی پروژه JPF [] پیاده سازی شده است.
9. برای اجرای نمادین برنامه‌های به زبان جاوا، ابزار SPF [] ارائه شده است. با استفاده از این ابزار می‌توان به صورت دلخواه مشخص کرد که چه تابع یا متغیری نمادین باشد. همچنین این ابزار از تعداد زیادی از حل کننده‌های قید پشتیبانی می‌کند که با استفاده از آنها می‌توان قیدهای مختلف را تحلیل کرد. به طور خاص برای رشته‌ها که در تحلیل ما بسیار اهمیت دارد، چند حل‌کننده قید با قدرت‌های مختلف در SPF وجود دارد. علاوه بر آن این ابزار اجرای Concolic را نیز پشتیبانی می‌کند و این موضوع باعث کشف تعداد بیشتری از خطاها در برنامه می‌شود. در این پژوهش با تغییر SPF به دنبال تشخیص آسیب‌پذیری تزریق به برنامک‌های اندرویدی هستیم.
10. ابزار LCT [8] ابزار متن باز روی جاوا است. در این ابزار سعی شده از معماری کارگذار-کارخواه[[10]](#footnote-10) برای ارتباط بین حل‌کننده قید و تحلیلگر استفاده کند. مشکل این ابزار این است که از چندنخی پشتیبانی نمی‌کند و توانایی پیدا کردن خطاهایی مثل کد روبه‌رو را ندارد. a[j]=1; if(a[i]!=0) ERROR;.
11. تحلیل کد برنامه، به تنهایی برای تحلیل کافی نیست. چون کد برنامه اطلاعی از مقادیر و چینیش داده ها در زمان اجرا ندارد. در مقابل تحلیل باینری مقیاس‌پذیر نیست و مفاهیمی مثل متغیرها ساختمان داده ها(آرایه ها و ..) در آن معنی ندارد. تنها با فریم های پشته و دستورات پرش و آدرس های حافظه سر و کار دارد. در AEG [9] از ترکیب هر دو روش یعنی تحلیل باینری و کد برنامه استفاده شده است. نحوه کار AEG به این صورت است:
    * ابتدا با استفاده از کد تحلیل نمادین صورت می گیرد تا به دستور آسیب‌پذیر برسد.
    * سپس شرط مسیر به حل کننده قید داده می شود تا ورودی مناسب تولید شود.
    * سپس به صورت پویا و با استفاده از ورودی تولید شده، فایل باینری برنامه تحلیل می شود تا اطلاعات زمان‌اجرا[[11]](#footnote-11) یعنی ساختار حافظه مثل آدرس بافر سرریز شده و آدرس بازگشت استخراج شود.
    * AEG قیدهای جدیدی مربوط به اطلاعات ساختار حافظه تولید می کند و به شرط مسیر اضافه می کند. این قیدها باید شامل shell code و آدرس بازگشت به shell code باشند. سپس شرط مسیر به حل کننده قید داده می شود تا ورودی مناسب تولید شود.
    * در نهایت AEG ورودی تولید شده را به برنامه می دهد تا بررسی کند که کد بهرجو[[12]](#footnote-12) آیا اجرا می شود یا نه! اگر حل کننده قید نتواند شرط مسیر را حل کند، AEG آن را رها می کند و فرایند را ادامه می دهد.

# فصل سوم نگارش صحيحنگارش صحيح

نگارش صحيح يك پایان نامه در فهم آسان آن بسيار موثر است. در اين فصل مهمترین قواعد نگارشی که باید مورد توجه جدی نگارنده قرار گیرد، به اختصار بیان می‌شود. اين قواعد را مي‌توان در محورهای اصلی زير دسته‌بندی کرد:

* فارسي‌نويسي
* رعایت املاي صحيح
* رعایت قواعد نشانه‌گذاري

## فارسي‌نويسي

در حد امكان سعی كنيد به جاي كلمات غير‌فارسی از معادل فارسی آنها استفاده كنيد، به‌ويژه در مواردی كه معادل فارسی مصطلح و رايج است‌.‌ به‌طور مثال استفاده از كلمه «لذا» به‌جای «برای همين» يا «به‌همين دليل» توجيهی ندارد‌. همچنين كلمه «پردازش» زيباتر از «پروسس» و معادل فارسی «ريز‌پردازنده» مناسب‌تر از «ميكروپروسسور» است‌.‌ در اين‌گونه موارد چنانچه احتمال عدم آشنايی خواننده با معادل فارسی وجود دارد، يا اصطلاح غير‌فارسی معمول‌تر است، در اولين ظهور كلمه فارسی، اصل غير‌فارسی آن به‌صورت پاورقي آورده شود‌.‌ اگر به‌ناچار بايد كلمات انگليسی در لابه‌لای جملات گنجانده شوند، از هر طرف يك فاصله بين آنها و كلمات فارسی پیش و پس از آنها در‌نظر گرفته شود‌.‌ چنانچه در پایان نامه از مختصر‌نويسی[[13]](#footnote-13) استفاده شود، لازم است در اولين استفاده، تفصيل آن در پاورقي آورده شود‌.‌

مثلاً: همگی می‌دانیم که از سیستم تعیین موقعیت فراگیر (GPS)[[14]](#footnote-14) می‌توان برای تعیین موقعیت جغرافیایی یک وسیله پرنده استفاده کرد.

## رعایت املاي صحيح فارسي

رعايت املاي صحيح فارسي به مطالعه و درك راحت‌تر كمك مي‌كند. همچنين در نوشته‌هاي فارسي بايد در حد امكان از همزه « ء، أ، ؤ، ة، إ، ئ» استفاده نشود‌.‌ به‌عنوان مثال «اجزاء هواپیما» و «آئين نگارش» ناصحیح، اما «اجزاي هواپیما» و «آيين نگارش» صحيح هستند.‌

## رعایت قواعد نشانه‌گذاري

منظور از نشانه‌گذاري به‌كار‌بردن علامت‌ها و نشانه‌هايي است كه خواندن و فهم درست یک جمله را ممکن و آسان مي‌كند. در ادامه نشانه‌هاي معمول و متداول در زبان فارسي و موارد کاربرد آنها به اختصار معرفی می‌شوند.

### ويرگول

ويرگول نشانه ضرورت یک مكث كوتاه است و در موارد زير به‌كار مي‌رود:

* در ميان دو كلمه كه احتمال داده شود خواننده آنها را با كسره اضافه بخواند، يا نبودن ويرگول موجب بروز اشتباه در خواندن جمله شود.
* در موردي كه كلمه يا عبارتي به‌‌‌‌عنوان توضيح، در ضمن یک جمله آورده شود. مثلاً برای کنترل وضعیت فضاپیماها، به‌دلیل آن‌که در خارج از جو هستند، نمی‌توان از بالک‌های آیرودینامیکی استفاده کرد.
* جدا‌كردن بخش‌هاي مختلف يك نشاني يا یک مرجع

پیش از ويرگول نبايد فاصله گذاشته شود و پس از آن يك فاصله لازم است و بيشتر از آن صحیح نیست.

### نقطه

نقطه نشانه پایان یک جمله است. پیش از نقطه نبايد فاصله گذاشته شود و پس از آن يك فاصله لازم است و بيشتر از آن صحیح نیست.

### دو نقطه

موارد كاربرد دونقطه عبارتند از:

* پيش از نقل قول مستقيم
* پيش از بيان تفصيل مطلبي كه به اجمال به آن اشاره شده‌است.
* پس از واژه‌اي كه معني آن در برابرش آورده و نوشته مي‌شود.
* پس از كلمات تفسير‌كننده از قبيل «يعني» و ...

پیش از دونقطه نبايد فاصله گذاشته شود و پس از آن يك فاصله لازم است و بيشتر از آن صحیح نیست.

### گيومه

موارد كاربرد گیومه عبارتند از:

* وقتي كه عين گفته يا نوشته كسي را در ضمن نوشته و مطلب خود مي‌آوريم.
* در آغاز و پايان كلمات و اصطلاحات علمي و يا هر كلمه و عبارتي كه بايد به‌صورت ممتاز از قسمت‌هاي ديگر نشان داده شود.
* در ذكر عنوان مقاله‌ها، رساله‌ها، اشعار، روزنامه‌ها و ...

### نشانه پرسشی

پیش از «؟» نبايد فاصله گذاشته شود و پس از آن يك فاصله لازم است و بيشتر از آن صحیح نیست.

### خط تیره

موارد كاربرد خط تیره عبارتند از:

* جدا‌كردن عبارت‌هاي توضيحي، بدل، عطف بيان و ...
* به‌جاي حرف اضافه «تا» و «به» بين تاريخ‌ها، اعداد و كلمات

### پرانتز

موارد كاربرد پرانتز عبارتند از:

* به‌معني «يا» و «يعني» و وقتي كه یک كلمه يا عبارت را براي توضيح بيشتر كلام بياورند.
* وقتي كه نويسنده بخواهد آگاهي‌هاي بيشتر (اطلاعات تكميلي) به خواننده عرضه كند.
* براي ذكر مرجع در پايان مثال‌ها و شواهد.

نکته: بین کلمه یا عبارت داخل پرانتز و پرانتز باز و بسته نباید فاصله وجود داشته باشد.

# فصل چهارم سبك ها و قلم ها سبك ها و قلم ها

در تعريف سبك‌هاي مختلف اين دستورالعمل از قلم‌هاي، B Nazanin و Times New Roman استفاده شده‌است كه خصوصيات كامل آنها‌ در بخش‌هاي بعدي تشريح مي‌گردد.

### قلم‌هاي فارسي

اندازه و سبك قلم‌هاي فارسي قابل استفاده در قسمت‌هاي مختلف يك گزارش در جدول ‏4-1 نشان داده شده‌است‌.‌

جدول 4-‌1 قلم‌هاي فارسي

|  |  |  |  |
| --- | --- | --- | --- |
| موقعيت استفاده از قلم | اندازه قلم | نام سبك | Bold |
| عنوان فصل | B Nazanin 20 | Heading1 | 🗸 |
| متن | B Nazanin 14 | Normal |  |
| زير‌فصل 1 | B Nazanin 18 | Heading 2 | 🗸 |
| زير‌فصل 2 | B Nazanin 16 | Heading 3 | 🗸 |
| زير‌فصل 3 | B Nazanin 14 | Heading 4 | 🗸 |
| زير‌فصل 4 | B Nazanin 13 | Heading 5 | 🗸 |
| زير‌فصل 5 | B Nazanin 13 | Heading 6 | 🗸 |
| عنوان جداول | B Nazanin 13 | Table Title\* | 🗸 |
| عنوان اشكال | B Nazanin 13 | Pic Title\* | 🗸 |
| متن جداول | B Nazanin 13 | In Table\* |  |
| متن جداول راست‌نويس | B Nazanin 13 | In Table R\* |  |
| متن اشكال | B Nazanin 13 | In Pic\* |  |
| مراجع (قسمت عادي) | B Nazanin 13 | FarsiRef\* |  |
| مراجع (قسمت پررنگ) | B Nazanin 13 | RefB\* | 🗸 |
| توضيحات كد برنامه‌نويسي | B Nazanin 11 | CodeComment\* |  |
| عنوان جداول پيوست | B Nazanin 13 | App Table Title\* | 🗸 |
| عنوان اشكال پيوست | B Nazanin 13 | App Pic Title\* | 🗸 |

### قلم‌هاي انگلیسی

اندازه و سبك قلم‌هاي انگلیسی قابل استفاده در قسمت‌هاي مختلف يك گزارش در جدول ‏4-2 نشان داده شده‌است‌.‌ اندازه قلم های انگلیسی یک شماره کوچکتر از فارسی می باشد.

جدول 4‌-‌2 قلم‌هاي انگلیسی.

|  |  |  |  |
| --- | --- | --- | --- |
| موقعيت استفاده قلم | اندازه قلم | سبك | Bold |
| متن | 13 Times New Roman | Normal |  |
| زير‌فصل 1 | 17 Times New Roman | Heading 2 | 🗸 |
| زير‌فصل 2 | 15 Times New Roman | Heading 3 | 🗸 |
| زير‌فصل 3 | 13 Times New Roman | Heading 4 | 🗸 |
| زير‌فصل 4 | 12 Times New Roman | Heading 5 | 🗸 |
| زير‌فصل 5 | 12 Times New Roman | Heading 6 | 🗸 |
| عنوان جداول | 12 Times New Roman | Table Title\* | 🗸 |
| عنوان اشكال | 12 Times New Roman | Pic Title\* | 🗸 |
| متن جداول | 12 Times New Roman | In Table\* |  |
| متن جداول راست‌نويس | 12 Times New Roman | In Table R\* |  |
| متن اشكال | 12 Times New Roman | In Pic\* |  |
| مراجع (قسمت عادي) | 12 Times New Roman | EnRef\* |  |
| مراجع (قسمت پررنگ) | 12 Times New Roman | RefB\* | 🗸 |
| توضيحات كد برنامه‌نويسي | 10 Courier New | CodeComment\* |  |
| كد برنامه‌نويسي | 10 Courier New | Code\* |  |
| كد برنامه‌نويسي (پر‌رنگ) | 10 Courier New | CodeBold\* | 🗸 |
| عنوان جداول پيوست | 12 Times New Roman | App Table Title\* | 🗸 |
| عنوان اشكال پيوست | 12 Times New Roman | App Pic Title\* | 🗸 |

## فرمول‌ها(روابط رياضي)

برای نوشتن روابط رياضی، ابزار Equation Editor از كارآيی خوبي برخوردار است‌.‌ تمامی نمادهای مورد‌نياز در اين ابزار پيش‌بينی شده‌است‌.‌ همچنین از شماره گذاری مناسب مطابق با فصل مذکور استفاده شود.

(‏4‌-‌1) 

(‏4‌-‌2) 

(‏4‌-‌3) 

در تنظيم قلم و سبك و اندازه فرمول‌ها از الگوي ارائه‌شده در جدول ‏4-3 و 4-4 پيروي مي‌شود. اين الگو با تنظيمات پيش‌فرض نرم‌افزار Word هماهنگي دارد.

جدول4‌-‌3 قلم و سبك فرمول‌ها.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| مثال | Italic | Bold | قلم | سبك | مورد كاربرد |
|  | 🗸 |  | Times New Roman | Variable | Variable |
|  | 🗸 |  | Times New Roman | Function | Function |
|  | 🗸 |  | Symbol | L.C.Greek | L.C.Greek |
|  |  |  | Symbol | U.C.Greek | U.C.Greek |
|  |  | 🗸 | Times New Roman | Matrix-Vector | Matrix-Vector |
|  |  |  | Times New Roman | Number | Number |
|  |  |  | Times New Roman | Text | Text |
|  |  |  | Times New Roman | Text | Constant Parameter |
|  |  |  | Times New Roman | Text | Unit |
|  |  |  | Symbol | Text | Math Operator |
|  |  |  | Times New Roman | Text | Math Function |

جدول 4-‌4 اندازه فرمول‌ها.

|  |  |
| --- | --- |
| Size | Position |
| 12pt | Full |
| 7pt | Subscript/Superscript |
| 5pt | Sub-Subscript/Superscript |
| 18pt | Symbol |
| 12pt | Sub-Symbol |

## فاصله‌هاي افقي و عمودي

تنظيم فاصله‌ها به خوانايي متن، تفكيك مناسب بخش‌هاي مختلف يك پایان نامه و زيبايي صفحات كمك مي‌كند..

### فاصله كلي از چهار طرف كاغذ

حاشيه از بالا 3 سانتي‌متر(2/1اینچ)،‌ از پايين 3 سانتي‌متر( 2/1اینچ)، از چپ 5/2 سانتي‌متر (1 اینچ) و از سمت راست كاغذ 3 سانتي‌متر(2/1 اينچ) در‌نظر گرفته مي‌شود‌.‌

### فاصله خط‌ها

فاصلة بين‌ خط‌ها بایستی 1.2 باشد.‌ كافي است اين كار يك بار روي سبك Normal اعمال گردد‌.‌

### فاصله‌هاي تفكيك‌كننده

با تنظيم فاصله‌ها مي‌توان تفكيك بخش‌هاي مختلف يك پایان نامه را ساده‌تر كرد تا هنگام مطالعه درك مطالب آسان‌تر باشد. برخي از فاصله‌هايي كه به‌منظور تفكيك بندها و عناوين به‌كار مي‌رود، به‌شرح زير مي‌باشد.

* پیش از هر بند يك فاصله عمودي به اندازه 6 pt قرار مي‌گيرد‌.‌ اين فاصله بايد به‌صورت دستي وارد شود.
* بند اول كه در زير عنوان آورده مي‌شود، از اول خط شروع شده و ساير بندها با 5 فاصله خالي از سر سطر شروع مي‌شوند‌.‌
* پیش از هر تيتر (بخش/ زير‌بخش/ زير‌زير‌بخش) يك فاصله عمودي به‌ترتيب به اندازه  
  (15/20/27 pt) قرار مي‌گيرد‌.‌ فاصله عمودي پیش از عنوان فصل، 30 pt مي‌باشد.

## فواصل بين كلمات

خيلي اوقات استفاده يا عدم استفاده از فاصله ضروري است كه در ادامه به مواردي از آن اشاره مي‌شود‌.‌

1. گذاشتن بيش از يك فاصله (Space) بين كلمات مجاز نمي‌باشد‌.‌ به‌عنوان مثال «اصول نگارش» صحيح، و «اصول نگارش» ناصحیح مي‌باشد‌.‌
2. پیش از عنوان اشكال و جداول و پس از شماره شكل يا جدول، دو فاصله خالي قرار مي‌گيرد.

## جدانوشتن كلمات بدون گذاشتن فاصله بين آنها

گاهي لازم است اجزاي يك كلمه از يكديگر جدا نوشته شوند، بدون آنكه بين آنها فاصله گذاشته شود (مثل كلمه «مي‌شود» يا «جدانوشتن»). به اين منظور بين دو بخش كلمه مورد نظر از <Ctr+-> يا <Shift+Space> (SS) استفاده كنيد.

تقريباً تمامي كلمات مركب در زبان فارسي بايد از هم جدا نوشته شوند؛ به استثناي صفات فاعلي مانند «عملگر»، «باغبان» و يا «دانشمند» و كلماتي نظير «اينكه»، «آنها».

## فهرست گزارش، فهرست شكل‌ها و فهرست جداول

اگر از اين الگو براي تهيه پایان نامه استفاده كنيد، پس از اتمام يا در حين تكميل آن مي‌توانيد با راست‌كليك روي فهرست فعلي، آن را به‌روز كنيد (توسط گزينه update field). فهرست جداول و اشكال نيز به‌همين صورت قابل به‌روز‌شدن مي‌باشد.

## سربرگ و ته‌برگ (Header and Footer)

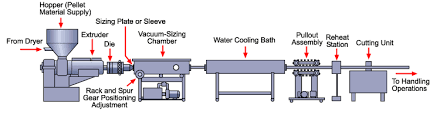
سربرگ و ته‌برگ را مي‌توان از منوي Insert انتخاب كرد‌.‌ به قاب‌هايي كه در قسمت بالا و پايين باز مي‌شود، به‌ترتيب سربرگ و ته‌برگ گفته مي‌شود‌.‌ در سمت راست سربرگ، عنوان هر فصل نوشته مي‌شود‌. در زير اين دو قسمت يك خط پررنگ قرار مي‌گيرد ‌و در ته‌برگ، شماره صفحه نوشته می شود.

## جداول، منحني‌ها، شكل‌ها

جداول و اشكال هر فصل بايد از شماره 1 به‌همراه شماره فصل مربوطه شماره‌گذاري‌ شود و در داخل متن (بلافاصله پس از بندي كه به آن شكل يا جدول ارجاع داده شده) آورده شود‌.‌ در متن بايد به تمامي جداول و شكل‌ها ارجاع داده شود‌.‌ در عنوان جداول و شكل‌ها نام كميت يا پديده مورد مطالعه ذكر مي‌شود.‌ عنوان جداول در بالای جدول و عنوان شکل در پایین ان ذکر گردد. (مشابه جدول 4-5 و شکل 4-1)

جدول4‌-‌5 عنوان جدول.

|  |  |  |
| --- | --- | --- |
| كار (WU) | زمان (ثانيه) | روش |
| 37/85 | 54 | چند شبكه‌اي |



شكل4‌-1 فرايند كواكستروژن.

## ارجاع به جداول، شكل‌ها، روابط، مراجع و بخش‌ها

* هرگز نبايد يك شكل يا جدول پيش از معرفی آن، در متن ظاهر شود‌.‌
* بين شماره شكل (يا جدول) و كلمه پیش از آن (شكل يا جدول) بايد حتماً يك فاصله قرار گيرد‌.‌ به‌عنوان مثال «شكل 2‌‌-‌‌2» صحيح، و «جدول2‌‌-‌‌2» ناصحیح است‌.‌
* براي ارجاع به شكل‌ها و جداول نبايد از پرانتز استفاده شود‌.‌ به‌عنوان مثال «جدول (2‌‌-‌‌2)» غلط است‌.
* ارجاع به روابط رياضی همواره بايد پس از درج خود آن روابط در متن صورت گيرد‌.
* برای ارجاع به روابط رياضی از شماره آنها در داخل پرانتز استفاده مي‌شود؛
* برای ارجاع به چند مرجع، آنها را با ويرگول جدا كنيد: [1، 2]

# فصل پنجم بررسي ساختار پایان نامهبررسي ساختار پایان نامه

به‌منظور استفاده از شيوه‌اي مناسب در تهيه يك پایان نامه، بايد روندي خاص دنبال شود. اين روند ممكن است تا حدودي شبيه به يك چک لیست ‌باشد، اما تبعيت از اين روند سبب مي‌شود در پايان گزارش‌نويسي، نيازي به صرف زمان فراوان براي ويرايش نهايي پایان نامه نباشد. از اين رو و به دليل اينكه ويرايش گزارش پایان نامه نياز به حوصله كافي دارد و در صورت استمرار، باعث كاهش حساسيت در رعايت ملزومات مي‌شود، به همین دلیل انجام ويرايش در پايان هر فصل، توصيه مي‌شود.

## بررسي سرفصل‌ها

پس از هر سرعنوان، لازم است كه متني هر چند مختصر نوشته شود. هيچ‌گاه پس از يك سرعنوان، نبايد بدون ظهور متن، سرعنوان داخلي شروع شود. در متن آغازين هر سرعنوان، لازم است كه محتواي فصل يا بخش و دليل وجود آنها، به‌منظور ايجاد فضاي ذهني در خواننده، بيان شود.

## بررسي ساختار كلي

بهتر است در صورت تشابه فصل‌هاي مختلف، از ساختار يكسان براي آنها استفاده شود. مثلا حالتي را در نظر بگيريد كه گزارشي براي متن يك برنامه نوشته مي‌شود. از آن‌جا كه معمولا برنامه از يك‌سري واحد تشكيل شده‌است، مي‌توان براي معرفي واحد‌ها، از ابتدا ساختار كلي تعريف كرد. مثلا ابتدا نقش واحد، سپس جايگاه آن در كل برنامه، پس از آن ساختار داخلي واحد، معرفي عمليات‌هاي داخلي و روابط پياده‌سازي‌شده و ... بيان شود.

## بررسي مفهومي

پس از اين كه ساختار‌دهي صورت گرفت و در ساختار ياد‌شده مطالب دسته‌بندي شد. مي‌توان نسبت به مطالعه مفهومي مطالب اقدام كرد.

## مطالعه مفهومي و جمله‌بندي

سعي شود هنگام مطالعه مفهومي به مباحث ويرايشي كمتر توجه شود و مفاهيم جملات، تعريف بندها، موقعيت بندها، بررسي صحت ارجاعات و مسايل مرتبط به مفهوم گزارش، مورد توجه قرار گيرد. بهتر است تصمیم‌گیری در مورد بندها مشخصا به‌عنوان يك قدم انجام شود.

## تنظیم بندها

بند اول كه در زير عنوان آورده مي‌شود، از اول خط شروع شده و ساير بندها با 5 فاصله خالي شروع   
مي شوند، تصمیم‌گیری در مورد بندها و تنظیم آنها، يكي از ملزومات اصلي يك گزارش پایان نامه است. به‌منظور انجام هوشمندانه اين كار، از تعريف خودكار فاصله‌دهي (Indentation) براي شروع بند جديد در الگو خودداري شده‌است. علاوه بر اين، با توجه به اينكه در گزارش‌نويسي فني، روابط رياضي زيادي مورد استفاده قرار مي‌گيرد، خودكارشدن فاصله‌دهي، باعث مي‌شود كه پس از هر رابطه، بند جديد در‌نظر گرفته شود كه وضعيت مطلوبي نمي‌باشد. بنابراين حين نوشتن، لازم است كه نويسنده به‌صورت هوشمندانه با قراردادن 5 فاصله خالي در ابتداي هر بند، آن را متمايز كند (به بند بعد توجه كنيد!).

بايد توجه داشت كه از قرار‌دادن شكل، در وسط يك بند خودداري ‌شود. بنابراين شكل‌ها بايد در انتهاي بند مربوطه آورده شود و حتما پس از شكل بايد بند جديد و با فاصله‌دهي بيان‌شده براي بند، شروع شود. در مجموع، به‌جز بندي كه بلافاصله پس از سرعنوان مي‌آيد، همواره يك بند بايد با 5 فاصله خالي، آغاز شود تا قابل تشخيص باشد.

به‌منظور زيبايي بيشتر پایان نامه، توصيه مي‌گردد در بين يك بند، شكل و يا جدول قرار نگيرد. با اين وجود پس از قرار‌گرفتن شكل يا جدول در ميان بندهاي يك سر‌فصل، بند پس از آن بدون فاصله ابتدايي آغاز مي‌گردد. چنانچه فرمولي نيز در ميان يك بند قرار مي‌گيرد، پس از درج فرمول، بند از ابتداي خط آغاز مي‌شود و نيازي به 5 فاصله خالي نيست.

## بررسي قواعد نگارشي

مطالعه مفهومي گزارش، ممكن است گاهي باعث تغيير در ساختار گزارش شود. بنابراين پس از اينكه بين مطالعه مفهومي و ساختار‌دهي، تعادل برقرار شد، مي‌توان نسبت به ويرايش گزارش اقدام كرد. به اين منظور لازم است كه يك بار گزارش پایان نامه بدون توجه به مفاهيم آن و فقط از نظر نگارشي مورد بررسي قرار گيرد. در اين راستا توجه به نكات زير حائز اهميت است:

1. فارسي‌نويسي
2. املاي صحيح
3. فواصل بين كلمات
4. موارد استفاده از Shift Space به‌جاي Space
5. نقطه‌گذاري، ويرگول‌گذاري و ...

## بررسي روابط

لازم است یک بار پایان نامه و برنامه های موجود به‌منظور بررسي مجدد صحت روابط، در مقايسه با مرجع مورد استفاده، مطالعه گردد. گاهي مشاهده مي‌شود كه در ماشين‌كردن روابط و حتي استخراج آن، خطا پديد مي‌آيد. با توجه به اينكه معمولا پس از استخراج روابط، از آنها در برنامه‌هاي رايانه‌اي استفاده مي‌شود، اين خطا به متن برنامه نيز كشيده مي‌شود. بنابراين بررسي صحت روابط از اهميت ويژه‌اي برخوردار است.

لازم است هنگام بررسي روابط، ارجاع‌دهي آنها نيز مورد توجه قرار گيرد. در يك گزارش فني لازم است كه روابط اصلي و نهايي كه در پياده‌سازي مورد استفاده قرار مي‌گيرد، به رابطه مشخصي در يك مرجع معتبر، ارجاع داده شود.

## بررسي شكل‌ها

بهتر است كل پایان نامه، يك بار فقط از منظر شكل‌ها مورد بررسي قرار گيرد. در اين بررسي، مي‌توان مواردي را كه در بخش‌هاي آتي تشريح مي‌شود، مورد توجه قرار داد.

### بررسي كيفيت شكل و تطابق عنوان آن

يكي از موارد مهم بررسي عناوين و تطابق آنها با شكل موردنظر مي باشد. همزمان با بررسي عنوان شكل، مي‌توان كيفيت آن را نيز مدنظر قرار داد.

### بررسي تطابق روابط، برنامه و شكل

در پروژه های پایانی كه به‌منظور تشريح متن يك برنامه نوشته مي‌شود، برخي از شكل‌ها به تشريح روابط پياده‌سازي‌شده اختصاص دارد. لازم است كه براي اين شكل‌ها، تطابق بين روابط موردنظر، مدل پياده‌سازي‌شده (متن برنامه) و شكل مربوطه مورد بررسي قرار گيرد.

## بررسي جداول

بهتر است كل پایان نامه، يك بار هم فقط از منظر جداول مورد بررسي قرار گيرد. در اين بررسي، مي‌توان مواردي را كه در بخش‌هاي آتي تشريح مي‌گردد، مورد توجه قرار داد.

### بررسي كيفيت جدول و تطابق عنوان آن

در اين بررسي لازم است كه بين محتويات جدول و عنوان آن تطابق برقرار باشد. هم‌زمان با بررسي عنوان جدول، مي‌توان كيفيت آن را نيز مدنظر قرار داد.

### بررسي تطابق روابط، برنامه و جدول

در پروژه های پایانی كه به‌منظور تشريح متن يك برنامه نوشته مي‌شود، برخي از جدول‌ها به تشريح روابط پياده‌سازي‌شده اختصاص دارد. بنابراين لازم است كه براي جداول، تطابق بين روابط موجود در گزارش فني، متن برنامه و روابط موجود در جدول، مورد بررسي قرار گيرد.

## به‌روز‌رساني مراجع

معمولا هنگام نوشتن پایان نامه به‌دليل توجه به متن مورد نگارش، ارجاع‌دهي مناسب مورد غفلت قرار مي‌گيرد. پس از اتمام نگارش مي‌توان براي هر فصل به بررسي ارجاع‌دهي پرداخت. در اين فعاليت لازم است تا با دقت فراوان بندهاي مختلف را مورد بررسي قرار داد و درصورت استفاده از مرجع خاصي، به آن ارجاع داده شود. در گزارش‌هاي فني لازم است كه روابط مهم و همچنين روابطي كه استخراج آن به‌صورت كامل در پایان نامه ارائه نشده‌است، ارجاع‌دهي شود. بهتر است در ارجاع‌دهي روابط، شماره رابطه مورد استفاده در مرجع موردنظر نيز ذكر گردد. مثلا (رابطه (3-2)، [3]). در بخش مراجع لازم است كه مراجع به‌ترتيب حضور در متن آورده شوند. مي‌توان اين مساله را در هر فصل به‌روز‌رساني كرد. اگر چه به‌روز‌رساني در انتهاي ويرايش تمامي فصول كفايت مي‌كند.

## صفحه‌بندي

پس از پايان اقدامات ويرايشي مختلف، مي‌توان با مرور كلي پروژه پایانی، نسبت به اصلاح صفحه‌بندي اقدام كرد. مثلا گاهي با جابه‌جاكردن يك شكل يا كوچك و بزرگ‌نمودن آن، مي‌توان صفحه‌بندي بهتري ارايه كرد. توجه داشته باشيد، با توجه به اينكه پس از صفحه‌بندي احتمالا شماره صفحات تغيير مي‌كند، اين اقدام پیش از بررسي سربرگ‌ها كه در بخش بعد تشريح مي‌شود، انجام شود.

## سربرگ و ته‌برگ‌ها

با توجه به استفاده از ابزار «Insert › Break» ، در پايان هر فصل، لازم است كه در آغاز هر فصل، موارد زير چك شود.

* عنوان فصل

عنوان فصل، در قسمت سمت راست بالاي صفحه قرار دارد و لازم است كه در هر فصل اصلاح شود.

* شماره صفحه

شماره صفحه، در پائين و وسط هر صفحه قرار دارد و لازم است در هر صفحه چک شود.

# فصل ششم جمع‌بندي و نتيجه‌گيري و پیشنهاداتجمع‌بندي و نتيجه‌گيري

در پايان گزارش‌هاي علمي و فني لازم است كه جمع‌بندي يا نتيجه‌گيري نهايي ارائه شود. در اين موارد مي‌توان آخرين فصل پایان نامه كه پیش از مراجع قرار مي‌گيرد را به اين امر اختصاص داد.

**پیشنهادات**

در این بخش پیشنهاداتی که محقق جهت ادامه تحقیقات دارد ارایه می‌گردد. دقت شود که پیشنهادات باید از تحقیق انجام شده و نتایج ان حاصل شده باشد و از ذکر جملات کلی باید پرهیز کرد.

# منابع و مراجع

|  |  |
| --- | --- |
| [1] | نام خانوادگی، نام (مولفان و مترجمان)؛ عنوان اصلی كتاب؛ عنوان فرعی كتاب (جزئيات عنوان كتاب در صورت وجود داخل پرانتز)، نام ساير افراد دخيل در تاليف يا ترجمه، ناشر، محل انتشار، شماره جلد، شماره ويرايش، سال انتشار به عدد‌.‌ |
| [2] | منهاج، محمد‌باقر؛ هوش محاسباتی (جلد اول: مبانی شبكه‌های عصبی)، انتشارات دانشگاه صنعتی امير‌كبير، تهران، ويرايش اول، 1379‌.‌ |
| [3] | نام خانوادگی، نام؛ نام‌‌خانوادگی و نام مولف دوم؛ مولف سوم؛ "عنوان مقاله به‌صورت عادي و داخل گيومه"، نام كامل مجله به صورت ايتاليك، شماره دوره يا جلد، شماره مجله، شماره صفحات، سال انتشار‌.‌ |
| [4] | نام خانوادگی، نام مجری؛ عنوان طرح پژوهشی به‌صورت ايتاليك، شماره ثبت، نام كامل محل انجام و سفارش دهنده، سال انجام طرح‌.‌ |
| [5] | نام شركت/ نام فرد؛ عنوان صفحه؛ آدرس اينترنتي. |
| [6] | Book authors’ names; Book Title in Italic (and the title components, if any), Edition number, Publisher, Date of publish. |
| [7] | Van de Vegte, J.; Feedback Control Systems, 2nd Edition, Prentice Hall, 1990. |
| [8] | Authors’ names separated by comma-dots; “The paper title in Regular Times New Roman 12pt”, Paper Address in Italic, Publishing Place, paper page, Year of Publish. |
| [9] | Safonov, M.; “Stability margins of diagonally perturbed multivariable feedback systems”, IEEE Proceedings, Part D, p. p. 251-256, Nov. 1982. |
| [10] | Company Name/ Person Name; Page Title; Internet Address. |

**يا بصورت الفبايي**

Gibson R.F "Principles of Composite Material Mechanics" Holman

J.P, Lloyd J.R (editors) McGraw-Hill (1994).

http:// 213.176.8.27/DL/Asklibraryian/FAQ/Theses.html.

Kantz H, Schreiber T "Nonlinear Time Series Analysis" 2nd ed.

Cambridge, Cambridge University Press (2004).

Minkowycz W.J, Roblach N.J, France D.M " Dynamic of Inert Gas

Bubbles in Force Convective Systems " Int J of Heat and Mass Transfer

Vol.24 (1981) PP 1433-1441.

Pagano N.J "Analysis of the Flexural Test of Bidirectional

Composites" J Composite Matter 1 (1967) pp 336-342.

Smith J.E "Biotechnology" 4th Ed New York, Cambridge University

Press (2004).

Soo S.L "Boundary Layer Motion of a Gas-Solid Suspension"

Proceeding of the Symposium on Interaction between Fluids and Particles,

Institute of Chemical Engineers Vol.1 (1962) PP 50-63.

Timoshinko S.P "Theory of Elastic Stability" McGraw-Hill, New

York (1985).

# پيوست‌ها

موضوعات مرتبط با متن گزارش پایان نامه كه در يكی از گروه‌های زير قرار می‌گيرد، در بخش پيوست‌ها آورده شوند:

1- اثبات های رياضی يا عمليات رياضی طولانی‌.‌

2- داده و اطلاعات نمونه (های) مورد مطالعه (Case Study) چنانچه طولانی باشد‌.‌

3- نتايج كارهای ديگران چنانچه نياز به تفصيل باشد‌.‌

4- مجموعه تعاريف متغيرها و پارامترها، چنانچه طولانی بوده و در متن به انجام نرسيده باشد‌.‌

براي شماره‌گذاري روابط، جداول و اشكال موجود در پيوست‌ از ساختار متفاوتي نسبت به متن اصلي استفاده مي‌شود كه در زير به‌عنوان نمونه نمايش داده شده‌است.

(پ-1) 

جدول پ-1: شرح كد منبع بدنه اصلي يك كد رايانه‌اي.

|  |
| --- |
| 01 program AeroPack;  02 uses  03 Forms,  04 Unit1 in 'Unit1.pas' {Form1},  05 Dialogs,  06 Sysutils;  07 {$R \*.res}  08 begin  09 Application.Initialize;  10 Application.Title := 'AeroPack';  11 Application.CreateForm(TForm1, Form1);  12 if pos('/h',Form1.Switches)<>0 then  13 begin  14 Application.ShowMainForm:=False;  15 Form1.Visible:=False;  16 end;  در صورتيكه سوئيچ /h در رشته سوئيچ موجود باشد، متغير ShowMainForm و خصوصيت Visible فرم اصلي را برابر با False قرار مي‌دهد. نتيجه اين كار عدم نمايش فرم اصلي خواهد بود.  17 Application.Run;  18 end. |

**Abstract**

This page is accurate translation from Persian abstract into English.

**Key Words:** Write a *3* to *5* KeyWords is essential.



Amirkabir University of Technology  
(Tehran Polytechnic)

… Department …

MSc or PhD Thesis

Title of Thesis

By

Name

Supervisor

Dr.

Advisor

Dr.

Month & Year

1. شروع مقدمه نبايد چنان طولاني باشد كه هدف اصلي را تحت‌ تاثير قرار دهد. [↑](#footnote-ref-1)
2. Path Condition [↑](#footnote-ref-2)
3. And [↑](#footnote-ref-3)
4. True [↑](#footnote-ref-4)
5. Execution Tree [↑](#footnote-ref-5)
6. Constraint Solver [↑](#footnote-ref-6)
7. Concrete [↑](#footnote-ref-7)
8. Random [↑](#footnote-ref-8)
9. Reliability [↑](#footnote-ref-9)
10. client-server [↑](#footnote-ref-10)
11. Runtime [↑](#footnote-ref-11)
12. Exploit [↑](#footnote-ref-12)
13. Abbreviation [↑](#footnote-ref-13)
14. Global Positioning System [↑](#footnote-ref-14)